MODI A LEAP TOWARDS SAE L4 AUTOMATED DRIVING FEATURES

A leap towards SAE L4 automated driving features

Book of Recommendations

31st August 2026



Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or CINEA. Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by the European Union

A leap towards SAE L4 automated driving features

Book of recommendations
31st August 2026

Document Summary Information

Grant Agreement No	101076810	**Acronym**	MODI
Full Title	A leap towards SAE L4 automated driving features		
Start Date	01/10/2022	**Duration**	48 months
Project URL	https://www.modiproject.eu		
Deliverable	D1.5 Book of recommendations		
Work Package	WP1 Requirements, business models and recommendations		
Contractual due date	30/09/2026	**Actual submission date**	31/08/2026
Nature	REPORT	**Dissemination Level**	PUB - Public
Lead Beneficiary	BAST		
Responsible Author(s)	Daniel Sander, Martin Thelen (BAST)		
Responsible Co-Author(s)	Julia Bräutigam, Ana M. Briele, Patrick Drossel (BAST); Lone-Eirin Lervåg (ITSN); Maria Backlund (LSP); Knut Jetlund (NMA); Trond H. Hovland (NPRA); Trond Foss, Gunnar Deinboll Jenssen (SIN); Ross Phillips (TOI),		
WP leader	Ross Phillips (TOI)		
Technical expert peer reviewer(s)	Tim Johannes (NMSH); Marianne Stølan Rostoft (NPRA); Claus Lund Andersen (VEJ)		
Quality peer reviewer(s)	Lone-Eirin Lervåg (ITSN)		
Approved	Ragnhild Wahl (ITSN)		



Revision history (including peer reviewing & quality control)

Version	Issue Date	% Complete	Changes	Contributor(s)
V0.1	27/07/2026	90	Draft for technical expert peer review	Daniel Sander, Martin Thelen (BAST)
V0.2	10/08/2026	99	Draft for quality review	Marianne Stølan Rostoft (NPRA); Tim Johannes (NMSH); Claus Lund Andersen (VEJ)
V1.0	31/08/2026	100	Final version (1.0)	Lone-Eirin Lervåg, Ragnhild Wahl (ITSN)

Disclaimer

The content of this document reflects only the author's view. Neither the European Commission nor CINEA is responsible for any use that may be made of the information it contains.

While the information contained in the documents is believed to be accurate, the author(s) or any other participant in the MODI consortium makes no warranty of any kind regarding this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

Neither the MODI Consortium nor any of its members, their officers, employees, or agents shall be responsible or liable in negligence or otherwise, howsoever in respect of any inaccuracy or omission herein.

Without derogating from the generality of the foregoing, neither the MODI Consortium nor any of its members, their officers, employees, or agents shall be liable for any direct or indirect or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

Copyright message

© MODI Consortium. This deliverable contains original, unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation, or both. Reproduction is authorized, provided the source is acknowledged.

Table of Contents

Executive Summary 9
1 Introduction 11
1.1 Project Summary 11
1.2 Aim of the Deliverable 12
1.3 Relation to MODI Output 12
1.4 Structure of the Report 13
1.4.1 How to Use the BoR 14
2 Methodology 15
2.1 Gathering Recommendations 15
2.2 Consolidation of Recommendations 18
2.3 Derivation of Recommendation Cards 19
3 Stakeholders 22
3.1 Enterprise View as Basis for Stakeholder Classification 22
3.2 Stakeholder Definition 22
4 MODI legacy: Advancing automated freight transport in Europe 26
4.1 MODI contributions to the European State of the Art 26
4.2 Supporting Europe's next generation of CCAM initiatives 28
4.2.1 Lessons learned from MODI deployment activities 29
5 Recommendations 34
5.1 Physical Infrastructure 34
5.2 Digital Infrastructure 43
5.2.1 Connectivity and Cooperative Services 44
5.2.2 Positioning and Mapping 53
5.2.3 Remote Operations 56
5.3 SAE Level 4 integration in logistics 62
5.4 Standardisation 84
5.5 International, European and National Regulations 100
6 Where to Start: Ten Priority Recommendations for Automated Freight Transport 111
6.1 Physical Infrastructure 111
6.2 Digital Infrastructure 112
6.3 SAE Level 4 Integration in Logistics 114
6.4 Standardisation 115
6.5 International, European and National Regulations 115
7 References 117
Annex I: Consolidated Recommendations 121
Annex II: Enterprise View on MODI Concept 143
Annex III: Trust, Human Factors and Public Acceptance in Level 4 Automated Freight Transport 156

List of Figures

Figure 1: Context of BoR in the overall MODI project 13
Figure 2: Methodology Flow Chart 16
Figure 3: Form for collecting partners' and stakeholders' recommendations 17
Figure 4: Example Recommendation Card 20
Figure 5: MODI's contribution to future European deployment of automated freight transport 33
Figure 6: Recommendation Card: Physical Infrastructure Readiness and Legibility 35
Figure 7: Recommendation Card: Cost-Effective and Staged Infrastructure Investment 37
Figure 8: Recommendation Card: Safety-Critical Support, Fallback and Special Sections 39
Figure 9: Recommendation Card: Confined Areas and Logistics-Site Readiness 41
Figure 10: Recommendation Card: Connectivity and Communication Continuity 45
Figure 11: Recommendation Card: Machine-interpretable Traffic Rules and Dynamic Road Data 48
Figure 12: Recommendation Card: Data Quality, Relevance and Feedback 51
Figure 13: Recommendation Card: Digital Maps, Positioning and Road Network 53
Figure 14: Recommendation Card: Logistics and Fleet Digital Integration 56
Figure 15: Recommendation Card: Digital Security and Trusted Processes 59
Figure 16: Recommendation Card: Deployment Strategy and ODD Definition 62
Figure 17: Recommendation Card: Operational Readiness and Safety Assurance 65
Figure 18: Recommendation Card: Remote Operation and Human Factors 67
Figure 19: Recommendation Card: End-to-End Logistics Integration and Vehicle Precision 70
Figure 20: Recommendation Card: Validation, Testing and Requirements Management 74
Figure 21: Recommendation Card: Business Models, Value Networks and Organisational Change 77
Figure 22: Recommendation Card: Trust, Public Acceptance and Human-Centred Communication 82
Figure 23: Recommendation Card: Taxonomies and Assessment Methods 85
Figure 24: Recommendation Card: V2X and C-ITS Communication Standards 87
Figure 25: Recommendation Card: Maps, Positioning and Corridor Data Standards 89
Figure 26: Recommendation Card: Vehicle–Infrastructure Interfaces and Traffic-Regulation Execution 91
Figure 27: Recommendation Card: Remote-Operation, Border and Enforcement Interfaces 94
Figure 28: Recommendation Card: Logistics, Terminal and Charging Process Standards 95
Figure 29: Recommendation Card: Interoperability, Open Standards and the Standards Landscape 97
Figure 30: Recommendation Card: Enterprise Model and Agreement Frameworks 99
Figure 31: Recommendation Card: Approval and Permit Frameworks 101
Figure 32: Recommendation Card: Liability and Legal Responsibility 103
Figure 33: Recommendation Card: Remote Operation Regulation 105
Figure 34: Recommendation Card: Safety Assurance and Regulatory Alignment 107
Figure 35: Recommendation Card: Data Governance and Cross-Border Procedures 109

Terms and Abbreviations

Term / Abbreviation	Description
5G	Fifth generation of cellular network technology
ADS	Automated Driving System
ANPR	Automatic Number Plate Recognition
API	Application Programming Interface
AVO	Automated vehicle owner
AVU	Automated vehicle user
BoR	Book of recommendations
CAM	Cooperative Awareness Message
CB	Certification body
C-ITS	Cooperative Intelligent Transport Systems
CCAM	Connected, cooperative and automated mobility
C-V2X	Cellular Vehicle-to-Everything
CEN	European Committee for Standardization
CPM	Cooperative Perception Message
DENM	Decentralized Environmental Notification Message
DI	Digital Infrastructure
DIA	Digital infrastructure authority
DoA	Description of Action
DSP	Digital service provider
eCMR	electronic Consignment Note
ERP	Enterprise Resource Planning
ETSI	European Telecommunications Standards Institute
FMS	Fleet Management System
GDPR	General Data Protection Regulation
GNSS	Global Navigation Satellite System
HD map	High-Definition Map
HMI	Human-Machine Interface
IRU	International Road Transport Union
ISO	International Organization for Standardization
ITS-G5	Intelligent Transport Systems - Wi-Fi standard IEEE 802.11p
KPI	Key Performance Indicator
L4	SAE Level 4 (of automation) / SAE Level 4 integration in logistics
LiDAR	Light Detection and Ranging
LTE	Long Term Evolution
MAPEM	Map Message
MCM	Manoeuvre Coordination Message
METR	Management of Electronic Traffic Regulations
MRM	Minimum Risk Manoeuvre
NDS	Navigation Data Standard
NRTK	Network Real Time Kinematic
OBE	On-Board Equipment
ODD	Operational Design Domain
OEM	Original Equipment Manufacturer
PDI	Physical and Digital Infrastructure
PI	Physical Infrastructure
PIA	Physical infrastructure authority
PIO	Physical infrastructure operator
PKI	Public Key Infrastructure
R&D	Research and Development

RC	Recommendation Card
Re	Regulation
RO	Remote Operator
RSE	Roadside Equipment
RVOS	Remote Vehicle Operation System
RWW	Road Works Warning
SAE	Society of Automotive Engineers
SAT	Site Assessment Test
SIR	Societal interest representative
SPATEM	Signal Phase and Timing Message
SRIDA	Strategic Research, Innovation and Deployment Agenda
SSP	Security service provider
St	Standardisation
TMS	Transport Management System
TOD	Target Operational Domain
TOS	Terminal Operating System
TSP	Transport service provider
TSU	Transport service user
TTP	Trusted Third Party
UC	Use case
UNECE	United Nations Economic Commission for Europe
V2X	Vehicle-to-Everything
VAM	Vulnerable road user Awareness Message
VM	Vehicle manufacturer
VMS	Variable message signs
VRU	Vulnerable Road User
WMS	Warehouse Management System
WP	Work Package

Executive Summary

The MODI project accelerates the introduction of highly automated freight vehicles by demonstrating complex real-life Connected, Cooperative and Automated Mobility (CCAM) use cases across a multi-country logistics corridor from Rotterdam to Oslo. The project investigates how SAE Level 4 automated trucks interact with logistics processes, infrastructure, digital services, regulatory frameworks and operational stakeholders across the complete freight transport system – not as isolated vehicle technology, but as an integrated logistics ecosystem. Five use cases demonstrate automated driving on public roads, automated terminal and port operations, automated loading and unloading, automated charging, digital customs procedures, gate access functions and remote supervision.

Key findings from the project demonstrate that SAE Level 4 automated freight transport cannot be treated as an isolated vehicle function. Successful deployment depends on the interaction between vehicles, infrastructure, digital services, logistics operators and public authorities, underpinned by common standards that enable interoperability, safety and regulatory harmonisation across the transport ecosystem. Large-scale reconstruction of existing road infrastructure is neither realistic nor necessary; current infrastructure can support automated driving provided that specific readiness issues are addressed selectively, such as lane marking quality, safe-haven areas and special infrastructure sections. Digital infrastructure emerges as a core enabler, with reliable connectivity, C-ITS services, high-accuracy positioning, HD maps, machine-interpretable traffic regulations and real-time road-event data being decisive for scaling automated freight operations beyond controlled environments. Cross-border automated freight operation is technically feasible but remains dependent on coordinated permit processes, aligned documentation, standardised interfaces and data exchange, clear allocation of operational responsibilities and reliable handover between national systems. Remote operation, remote assistance and human-system interaction are central elements of Level 4 freight deployment, with human factors needing to be addressed early in the system design. The business value is not created solely by replacing the driver but by combining automated driving with digitalised logistics processes, predictable operations, standardised interfaces and new forms of cooperation across the logistics chain. Accordingly, contributions to European and international standardisation—including standards supporting interoperability, certification, safety, cybersecurity and digital integration—are a strategic prerequisite for scalable, cross-border deployment of SAE Level 4 freight transport and therefore constitute a central pillar of the MODI Book of Recommendations.

This deliverable presents 90 consolidated recommendations organised into 30 recommendation cards across five thematic areas: Physical Infrastructure, Digital Infrastructure, SAE Level 4 Integration in Logistics, Standardisation, and Regulation. Each card identifies relevant stakeholders, main challenges, recommended actions and an indicative deployment horizon.

The ten priority recommendations – in a shortened version – are:

1. Establishing CCAM-ready infrastructure assessment criteria for corridors, ports, terminals and logistics hubs
2. Aligning public-road and confined-area infrastructure requirements to avoid operational discontinuities
3. Providing traffic rules and regulations in digital, cybersecure machine-interpretable formats
4. Ensuring reliable and standardised connectivity along automated freight corridors including cross-border continuity
5. Prioritising early deployment on high-volume, predictable point-to-point routes with simple, well-defined Operational Design Domains
6. Designing automated freight vehicles as part of an end-to-end logistics system including loading, unloading, charging and yard processes
7. Requiring interoperability across OEMs, infrastructure providers, map providers, logistics systems and countries before large-scale deployment
8. Aligning vehicle and infrastructure, remote-operation, terminal, gate, charging and logistics interfaces with existing standards
9. Harmonising permit processes across Europe including parallel applications and mutual recognition of safety assessments
10. Clarifying liability and responsibility by distinguishing traffic-safety liability from cargo-related liability across all actors

The recommendations are grounded in an Enterprise View that defines twelve enterprise objects, the Societal Interest Representatives and their relationships through expectations and agreements, providing common terminology and supporting a European one-to-all interaction model instead of fragmented bilateral arrangements.

Three annexes provide additional detail on all consolidated recommendations with traceability, the Enterprise View stakeholder framework, and trust, human factors and public acceptance considerations.

MODI demonstrates that automated freight deployment requires coordinated progress across vehicle technology, infrastructure, digital services, logistics operations, regulation and stakeholder governance.

The Book of Recommendations provides strategic, practical and harmonised guidance for policymakers, industry stakeholders, infrastructure operators and regulatory bodies to support the broader deployment of CCAM freight solutions beyond the project's lifetime.

1 Introduction

This deliverable provides recommendations on five topics relevant for SAE Level 4 freight transport: physical and digital infrastructure, operational aspects, standardisation and regulation. Lessons learned from the tasks conducted in MODI are also presented.

1.1 Project Summary

MODI Ambitions: A leap towards SAE L4 automated driving features

The MODI project aims to accelerate the introduction of highly automated freight vehicles through demonstrations and by overcoming barriers to the rollout of automated transport systems and solutions in logistics. The logistics corridor from the Netherlands to Norway has been chosen for demonstration activities as the Netherlands, Germany, Denmark, Sweden, and Norway are expected to be among the first movers to implement fully automated vehicles in Europe.

MODI comprises five use cases, each describing a part of the logistics chain in confined areas and on public roads. It identifies what is already possible on an automated driving level without human interaction and what is yet to be developed. The MODI objectives are to:

- Implement new technology within the Cooperative, Connected and Automated Mobility (CCAM) spectrum.
- Define recommendations for the design of physical and digital infrastructure.
- Demonstrate viable business models for connected and automated logistics.
- Perform technical and socio-economic impact assessments.

Major challenges include regulatory aspects and standardisation, border crossings, access control, charging, coordination with automated guided vehicles, loading/unloading and handover from the public to confined areas.

MODI test sites include a CCAM test corridor from Rotterdam to Oslo with specific use cases at Rotterdam (The Netherlands), Hamburg (Germany), Gothenburg (Sweden), and Moss (Norway).

The ambition of MODI is to take automated driving in Europe to the next level by demonstrating complex real-life CCAM use cases while:

- Showing the local, national, and international context of freight transport with CCAM vehicles, both in confined areas and on public roads.
- Cooperating and co-creating with logistics companies, road operators, vehicle OEMs, providers of physical and digital infrastructure and other stakeholders to bridge the gap between R&D and market readiness.
- SAE Level 4 solutions for long-distance operational design domains.
- Creating innovative business models and improved business models across the logistics chain.
- Proving that the technology can soon deliver on promised benefits at relatively high speeds and medium traffic complexity, including a coordinated CCAM system to support smart traffic management.
- Paving the way to enable highly automated transport on important corridors, connecting main ports across Europe.
- Accelerating CCAM in Europe by setting examples of business-wise CCAM integration in logistics.

1.2 Aim of the Deliverable

The aim of this deliverable is to contribute directly to Objective 2 of the MODI project, which focuses on defining recommendations for the adaptations required to enable the broader deployment of CCAM solutions in freight transport. In line with the Grant Agreement, the deliverable identifies the necessary changes to supporting infrastructure, regulatory frameworks and relevant standards, with the overarching goal of accelerating the introduction of automated vehicles and informing future large-scale deployment activities. Therefore, the work presented here consolidates the project's insights into three main areas:

1. recommendations for adapting physical and digital infrastructure;
2. lessons learned for the introduction of SAE Level 4 CCAM vehicles in freight logistics; and
3. the harmonisation of European vehicle regulations, UN regulations, and the relevant national behavioural laws in the participating countries.

1.3 Relation to MODI Output

This deliverable is closely interlinked with the overall structure and output strategy of the MODI project. As the Book of Recommendations (BoR), it represents the project's central legacy document and consolidates the key insights, lessons, and strategic directions that have emerged across all work packages (WPs). While the preceding work provides the analytical, technical, regulatory, and operational foundations, this report synthesises and further develops these diverse inputs into a set of recommendations aimed at supporting the deployment of large-scale CCAM freight operations.

The development of the BoR has been inherently cross-cutting, drawing systematically on the results generated throughout the project. WP1 contributes the fundamental requirements and business model considerations, forming the basis for understanding operational needs and stakeholder expectations. WP2 provides the gap and impact assessments that highlight the barriers and opportunities for deployment, thereby shaping the prioritisation of recommendations. WP3 contributes with vehicle-related insights, including technical, functional, and safety aspects that must be reflected in both regulatory and infrastructural recommendations.

In addition, WP4 delivers essential findings on the physical and digital infrastructure adaptations required to support automated freight transport at scale. WP5 brings in practical evidence from use cases, ensuring that the recommendations reflect real operational contexts and lessons learned from demonstrations. WP6 contributes with innovation insights and forward-looking perspectives, helping to ensure that the recommendations remain relevant beyond the immediate project scope.

The BoR has been developed through a collaborative, iterative process involving the BoR Core Team and the active participation of all MODI partners, as illustrated in Figure 1. This process ensured that the document integrates insights from technical, operational, regulatory, and innovation domains rather than simply summarizing project activities.

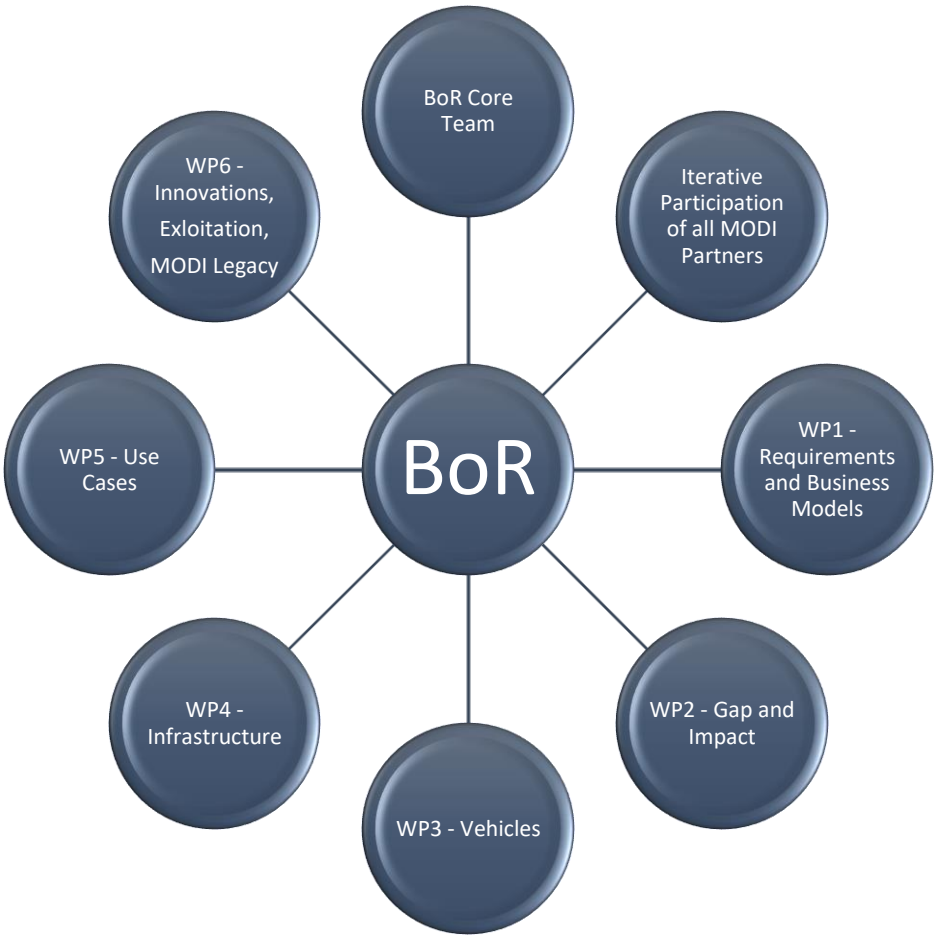


Figure 1: Context of BoR in the overall MODI project

As such, this report stands as one of the key project outputs intended to guide policymakers, industry stakeholders, infrastructure operators, and regulatory bodies. It provides strategic, practical, and harmonised recommendations that reflect the collective knowledge generated within MODI, ensuring that the project's outcomes continue to support the broader deployment of CCAM freight solutions beyond the project's lifetime.

1.4 Structure of the Report

This report is organised to guide the reader logically through the objectives, context, and outcomes of the MODI project. It begins with an Executive Summary, providing a concise overview of the key findings and recommendations. Chapter 1 introduces the project, outlining its background, summarising its purpose, and explaining the aim of the deliverable. It also clarifies how this document relates to the broader MODI outputs before concluding with an overview of the report's structure.

Chapter 2 details the methodology behind the Book of Recommendations. It explains how inputs from multiple sources (surveys, deliverables, interviews) were gathered, systematically consolidated, and organised into 90 evidence-based recommendations grouped by thematic area.

Chapter 3 presents the relevant stakeholders, establishing the roles and perspectives that shape the project environment.

This is followed by Chapter 4, which highlights how MODI creates value for the involved actors and the wider ecosystem.

Chapter 5 contains the core recommendations, organised into five thematic areas. It opens with physical infrastructure, addressing corridor-wide baseline conditions. The subsequent section on digital infrastructure is structured into three subsections covering European C-ITS standards for automated driving, positioning and mapping, and remote operations. The third thematic area addresses the integration of SAE Level 4 CCAM vehicles in freight transport and encompasses topics such as deployment strategy and Operational Design Domain (ODD) definition, operational readiness and safety assurance or remote operation. The chapter then turns to standardisation, examining harmonisation needs for SAE Level 4 automated freight transport. The final section addresses applicable international, European and national regulations, with particular focus on approval and permit frameworks, liability allocation and the harmonisation of regulatory processes across jurisdictions.

Chapter 6 provides the 10 key recommendations with the highest relevance according to the project partners.

The document is supplemented by 3 annexes, which include additional material, offering further detail and supporting information for readers who require deeper insight into these areas.

1.4.1 How to Use the BoR

Chapter 5 presents the full set of 90 MODI recommendations, organised into 30 recommendation cards across five thematic areas: physical infrastructure, digital infrastructure, SAE Level 4 integration in logistics, standardisation, and regulation. Each card summarises the main challenges, identifies the relevant stakeholders, groups related recommendations, and indicates an estimated implementation horizon. Readers can therefore consult the thematic sections most relevant to their role or area of interest.

Chapter 6 provides the conclusion section and a more focused entry point for implementation. It highlights two priority recommendations from each thematic area – ten recommendations in total – that MODI partners consider particularly important for accelerating the deployment of Level 4 CCAM freight transport in European logistics. Readers looking for practical guidance on where to begin should start with this chapter before consulting the more detailed recommendations in Chapter 5.

2 Methodology

The methodology for developing the BoR was designed to ensure that the final output reflects the full breadth of knowledge, experience, and evidence generated across the MODI project. As a cross-cutting deliverable, the BoR builds on the results of all preceding work packages and MODI use cases, and its content has been shaped through a collaborative process involving the entire consortium.

The work followed a multi-stage approach. First, the findings produced within the technical and analytical work packages were reviewed, consolidated, and organised in line with the five thematic areas defined in the Description of Action (DoA): Physical Infrastructure (PI), Digital Infrastructure (DI), SAE Level 4 integration in logistics (L4), Standardisation (St), and Regulation (Re). This provided the conceptual framework within which recommendations could later be systematically collected and aligned.

2.1 Gathering Recommendations

In total the deliverable used as inputs:

- 24 survey questionnaires,
- 14 MODI deliverables,
- 3 information notes that were not official deliverables but created during the work in different work packages and
- Discussions and collaborative workshops held at the 2024 consortium meeting, followed by interviews with relevant project partners and documented insights from the core team bi-weekly meetings

From these inputs, 30 recommendation cards and the top 10 recommendations of MODI are derived as shown in Figure 2.

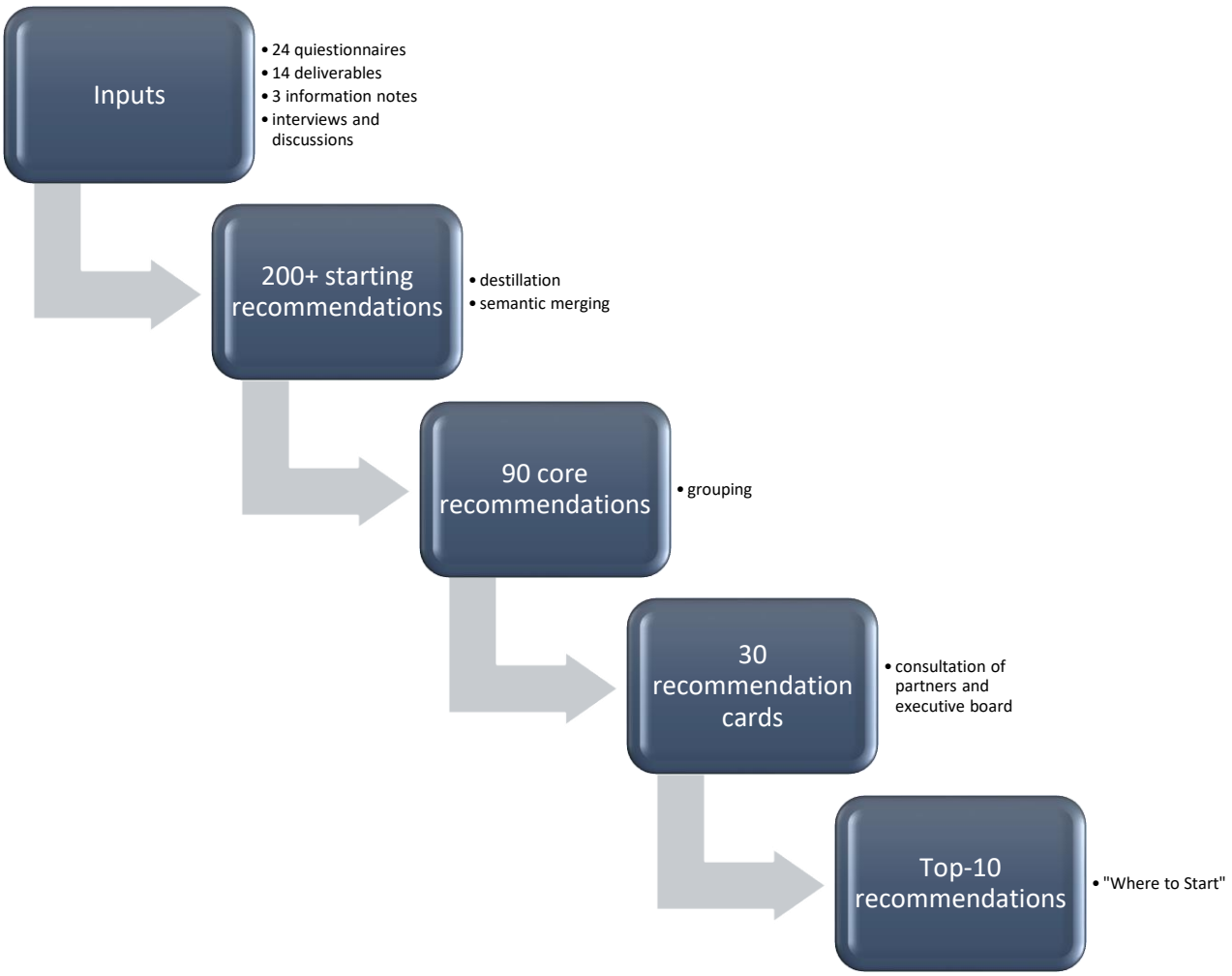


Figure 2: Methodology Flow Chart

MODI Consortium

A central component of the methodology was a questionnaire distributed to all MODI partners. The questionnaire served as a structured mechanism to gather recommendations directly from the organisations involved in the project's research, demonstrations, and analysis. Each partner was invited to submit up to ten recommendations, each consisting of two elements:

- a concise one-sentence recommendation; and
- a short motivation text of three to four sentences explaining its rationale, context, and relevance.

For each recommendation, contributors were asked to indicate whether the proposal related to a specific WP and/or Use Case (UC), thereby supporting traceability to the project's evidence base. Furthermore, each entry had to be classified under one or more of the five DoA topics (PI, DI, L4, St, Re), ensuring thematic consistency and enabling systematic aggregation across contributions. The questionnaire template is illustrated in Figure 3.

No.	Context	Description	Classification				
			PI	DI	L4	St	Re
1	**UC** Select UC **WP** Select WP	**Recommendation** (*1 sentence*): Write one sentence here	☐	☐	☐	☐	☐
		Motivation (*3-4 sentences*): Write three to four sentences here					
2	**UC** Select UC **WP** Select WP	**Recommendation** (*1 sentence*): Write one sentence here	☐	☐	☐	☐	☐
		Motivation (*3-4 sentences*): Write three to four sentences here					
3	**UC** Select UC **WP** Select WP	**Recommendation** (*1 sentence*): Write one sentence here	☐	☐	☐	☐	☐
		Motivation (*3-4 sentences*): Write three to four sentences here					
.....							
10	**UC** Select UC **WP** Select WP	**Recommendation** (*1 sentence*): Write one sentence here	☐	☐	☐	☐	☐
		Motivation (*3-4 sentences*): Write three to four sentences here					

Legend: DoA classification

PI Physical Infrastructure
DI Digital Infrastructure
L4 Best Practices for L4 CCAM
St Standardization
Re Regulation

Figure 3: Form for collecting partners' and stakeholders' recommendations

MODI Deliverables and Reports

To ensure that the BoR is grounded not only in partner judgement but also in the documented results of the project's technical, operational and analytical work, the questionnaire responses were complemented by a systematic review of relevant MODI project deliverables. From these deliverables, explicit recommendations and recommendation-like statements were extracted and incorporated into the evidence base. These included explicit recommendations as well as normative statements contained in sections such as conclusions, lessons learned, best practices, future work, validation results and use case findings. These deliverable-based inputs were reviewed against the same five thematic areas and then compared with the questionnaire-derived recommendations. As the deliverables generally did not contain structured motivation fields, they were treated primarily as evidence and contextual support rather than as sources of original motivation texts like in the questionnaire. Where deliverable findings confirmed or strengthened an existing consolidated recommendation, the relevant source reference was added to that recommendation. Where a deliverable introduced a distinct and previously uncovered issue, a new consolidated recommendation was created.

2.2 Consolidation of Recommendations

Following the data collection phase, all submitted recommendations were compiled into a common working database and reviewed by the BoR core team. As several partners addressed similar challenges from different professional, technical, operational or regulatory perspectives, a structured consolidation process was required to avoid duplication while preserving the substance of the original input.

The consolidation followed a semantic rather than purely textual approach. Recommendations were therefore not considered duplicates only when they used identical wording, but also when they addressed the same underlying issue, proposed the same type of action, or pointed to the same implementation need. For example, recommendations referring to harmonised vehicle–infrastructure interfaces, logistics system APIs (Application Programming Interfaces), terminal access interfaces or digital mission-management interfaces were assessed together, even where they originated from different work packages or use cases. Similarly, recommendations concerning safe fallback areas, Minimal Risk Manoeuvres (MRMs) –automated procedures to bring a vehicle to a safe state in case of system failure as, for instance, defined in [8] – recovery locations or operational stop areas were grouped where they addressed the same infrastructure function.

Each recommendation was assessed against four main criteria:

1. **Substantive meaning** – whether the recommendation addressed the same underlying need or problem as another recommendation.
2. **Operational function** – whether it contributed to the same deployment capability, such as remote operation, digital traffic management, automated gate access, map updates or safety validation.
3. **Thematic fit** – whether it belonged primarily to one of the five DoA thematic areas: Physical Infrastructure, Digital Infrastructure, SAE Level 4 Integration in Logistics, Standardisation or Regulation.
4. **Level of abstraction** – whether it represented a general strategic recommendation, a specific implementation measure, or an example supporting a broader recommendation.

Where two or more recommendations expressed the same core message, they were merged into a single consolidated recommendation. In doing so, it was aimed to retain the most complete and transferable formulation. The final wording was usually written at a higher level of abstraction than the individual source statements, so that it could apply across multiple use cases, countries, stakeholders and deployment contexts. At the same time, overly broad formulations were avoided where a specific technical or regulatory issue was considered important for implementation.

Where recommendations were similar but not identical, the team distinguished between full duplicates, partial overlaps, and complementary recommendations. Full duplicates were merged directly. Partial overlaps were merged where their main policy or implementation message was the same, with specific aspects retained through the source references, motivation texts or explanatory notes. Complementary recommendations were kept as separate entries if they addressed different aspects of deployment, for example where one recommendation concerned physical infrastructure readiness, and another concerned digital interface standardisation.

This process aimed to ensure that the final recommendation list would be concise and usable, while still reflecting the diversity of partner input. Another aim was to prevent the final BoR from being dominated by repeated statements on the same topic, while at the same time ensuring that recurring themes would be recognised as important.

The questionnaire asked contributors to provide not only a one-sentence recommendation, but also a short motivation text explaining the rationale behind the recommendation. These motivation texts were treated as an important part of the evidence base, as they often explained why a recommendation was relevant, which operational problem it addressed, and how it related to specific MODI use cases or work package findings.

During consolidation, original motivation texts were retained and mapped to the consolidated recommendation that they supported. Where several original recommendations were merged into a single consolidated recommendation, their motivation texts were also associated with the same final recommendation ID. This means that one consolidated recommendation can have multiple underlying motivation texts.

2.3 Derivation of Recommendation Cards

The 90 consolidated recommendations are not presented individually in Chapter 5. Instead, they are organised into thematic clusters and displayed through a standardised format called a recommendation card. Each card groups a set of closely related consolidated recommendations that address a common operational challenge, functional capability, or governance requirement.

The card format was chosen to make the recommendations accessible to a diverse audience while preserving traceability to the underlying evidence and making explicit which stakeholder groups each cluster concerns. Each recommendation card of Chapter 5 is dedicated to one thematic area, and thus are numbered sequentially within their area (e.g., RC-PI-1 for the first card in Physical Infrastructure, RC-DI-3 for the third in Digital Infrastructure).

Each recommendation card consists of two components: a structured header table and a narrative synthesis. The header table comprises five rows:

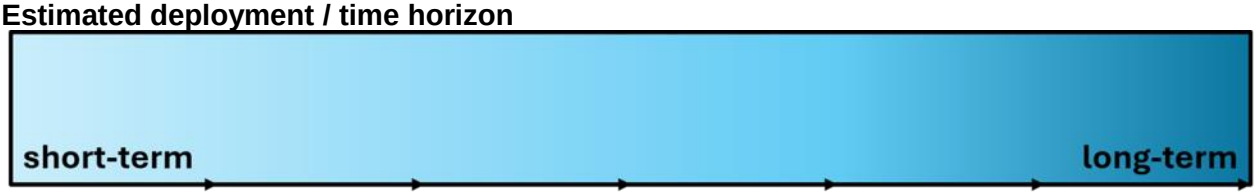
Identifier	**Title**												
Stakeholder	*AVO*	*AVU*	*CB*	*DIA*	*DSP*	*PIA*	*PIO*	*RO*	*SSP*	*TSP*	*TSU*	*VM*	*SIR*
Main Challenges Addressed: • Aa • Bb • Cc ….													
Recommendations • XY-1 • XY-2 • XY-3 …													
Estimated deployment / time horizon 													

Figure 4: Example Recommendation Card

- **Card identifier and title:** Each card is assigned a unique alphanumeric identifier (e.g., RC-PI-2, RC-L4-5) in which the letter code denotes the thematic area (PI = Physical Infrastructure, DI = Digital Infrastructure, L4 = L4 Integration in Logistics, St = Standardisation, Re = Regulation) and the number indicates the card's position within that area. The title describes the functional or policy focus of the bundled recommendations.
- **Stakeholders:** This row lists the twelve enterprise objects and Societal Interest representatives defined in the stakeholder definition (chapter 3.2: AVO, AVU, CB, DIA, DSP, PIA, PIO, RO, SSP, TSP, TSU, VM, SIR) and marks those primarily addressed by the card's recommendations. The row allows stakeholder-specific readers to quickly identify the recommendation clusters of direct relevance to their role. One card may address several stakeholder groups simultaneously where the required actions are distributed across actors. Relevant stakeholders are highlighted in black font.
- **Main challenges addressed:** This row states the operational, technical, regulatory, or governance problems to which the bundled recommendations respond. It frames the deployment barrier in concrete terms and provides the problem logic from which the recommendations derive their rationale.
- **Recommendations:** This row lists the individual consolidated recommendations that are grouped in the card, each identified by the unique recommendation ID assigned during consolidation (e.g., PI-03, DI-07, L4-14). These are the statements produced through the process described in the preceding section. The full wording of all consolidated recommendations, together with source references and motivation texts, is provided in Annex I.

- **Estimated deployment / time horizon**: The time horizon indicates the period within which the recommendations grouped in a card could realistically be initiated, advanced or implemented after the publication of this BoR. To make the assessment more transparent, the following time ranges are used:
    - short term refers to measures that can be addressed within 0–2 years after publication;
    - medium term refers to measures requiring approximately 2–5 years; and
    - long term refers to measures requiring approximately 5–10 years.

  Where a card combines categories, such as short-to-medium or medium-to-long term, the corresponding combined range is used.

  Short-term measures are typically those that can be started with existing instruments, limited investment, pilot experience, organisational preparation or near-term regulatory steps. Medium-term measures usually require coordinated infrastructure investment, standardisation work, digital service development, stakeholder alignment or legislative preparation. Long-term measures refer to structural changes that depend on extended regulatory cycles, large-scale investment, mature interoperability frameworks, harmonised governance models or broad market and societal uptake.
  The time horizons are not fixed implementation deadlines. They are indicative ranges and may vary depending on national context, infrastructure maturity, regulatory readiness, stakeholder capacity and the operational domain of the specific deployment environment.

The narrative synthesis follows the header table and elaborates the card's content in discursive form. It contextualises the bundled recommendations within MODI's evidence base, explains the rationale for their grouping, and draws on findings from project deliverables and stakeholder questionnaire inputs to substantiate each recommendation. The narrative also identifies relationships between the individual recommendations within the card and, where relevant, situates them in relation to existing standards, regulations, or prior research, so that what is proposed as new, extended, or adapted is clearly distinguishable from what is already addressed.

3 Stakeholders

The deployment of SAE Level 4 CCAM vehicles in freight transport involves a set of interacting actors that jointly form the operational, organisational and contractual environment of automated logistics. In the MODI context, these actors include organisations, authorities, companies, service providers and other legal entities that may own, operate, supervise, certify, regulate, secure or use automated transport services. The stakeholder description in this chapter is based on an Enterprise View, which defines stakeholders as “enterprise objects” and describes their relationships through expectations and agreements [4].

The purpose of this chapter is to provide a common stakeholder terminology for the BoR. This terminology is used in Chapter 5 to describe which stakeholder groups are relevant for the consolidated recommendations. In line with the Enterprise View, one legal entity may fulfil the responsibilities of more than one enterprise object. For example, a company may provide transport services while also being the owner and user of an automated vehicle.

3.1 Enterprise View as Basis for Stakeholder Classification

The MODI stakeholder classification follows an Enterprise View approach. The Enterprise View is based on the ARC-IT architecture used in ISO TC 204 ITS architecture documents [4] and complements physical, functional and communication views by focusing on enterprise objects and their relationships. In this context, enterprise objects can be persons, organisations, companies, authorities or other types of stakeholders.

The Enterprise View distinguishes two main types of relationships between enterprise objects: expectation relationships and contractual relationships. Expectation relationships describe the information or services that one enterprise object expects from another. Contractual relationships describe agreements between enterprise objects and may differ between regions, countries and use cases. The Enterprise View may also describe how an enterprise object interacts with physical resources, for example by owning, operating, developing, installing or maintaining them.

For the BoR, the enterprise objects defined in the MODI Enterprise View are used as the consolidated stakeholder groups. This avoids introducing a separate stakeholder taxonomy and supports consistency between the stakeholder chapter, the recommendations on roles and responsibilities, and the recommendations on standardised relationships and agreement frameworks.

3.2 Stakeholder Definition

The following entities form the stakeholder basis for the BoR and will be used as stakeholder labels in the recommendation cards. The interconnection according to the Enterprise View is depicted in “Figure 1: The complete Enterprise View of the MODI concept” of Annex II.

- **Automated vehicle owner (AVO)** owns the automated vehicle. The Automated vehicle owner could also be the Automated vehicle user. Examples of legal entities being Automatic vehicle owners are a natural person or a legal entity, including companies, public authorities, and non-profit organizations, provided that the owner can be uniquely identified and held legally and financially responsible.

Examples: a logistics company that owns its automated truck fleet, a vehicle-leasing company, or a public authority that owns automated service vehicles

- **Automated vehicle user (AVU)** uses the automated vehicle for his/her own purposes or for providing transport services like transport of persons and goods. The Automated vehicle user could also be the Automated vehicle owner. Examples on legal entities being Automatic vehicle users are a natural person or a legal entity, including companies, public authorities, and non-profit organizations, provided that the user has an owner-user agreement with the Automated Vehicle Owner in those cases where the owner and user is not the same legal entity.

  Examples: a carrier operating automated trucks for freight transport, a terminal operator using automated vehicles on its premises, or another organisation authorised by the vehicle owner to use the vehicle.

- **Certification body (CB)** is an entity that is authorised by a physical and/or a digital authority, or any other relevant authority, to certify the relevant Enterprise, Physical and Functional objects.

  Examples: an accredited technical service, inspection organisation, or conformity-assessment body authorised to assess and certify vehicles, operators, infrastructure components, or digital services.

- **Digital infrastructure authority (DIA)** is a legal entity that develops, manages and publish laws, regulations and guidelines for the use of digital infrastructure governed by the authority, e.g. infrastructure used for communication and positioning services related to automated vehicles. Examples on Digital infrastructure authorities are Communication authorities, Data Protection Authority, Map authorities, Positioning systems authorities, electronic traffic rules and regulation authorities and Road authorities that e.g., manages national road data bases.

  Examples: a national telecommunications regulator, data-protection authority, mapping or geodetic authority, and a road authority responsible for authoritative digital road or traffic-regulation data.

- **Digital service provider (DSP)** is an entity that supports other Enterprise objects with digital services needed for their fulfilment of responsibilities. A Digital service provider is often authorised by a digital infrastructure authority to provide digital services.

  Examples: a mobile network operator, GNSS correction-service provider, HD map provider, C-ITS service provider, cloud-service provider, or digital traffic-information provider.

- **Physical infrastructure authority (PIA)** is a legal entity that develops, manages and publish regulations and guidelines for the use of physical infrastructure governed by the authority, e.g. infrastructure used for transport of goods and persons on roads and infrastructure for vehicles in confined areas, e.g., terminals and harbours. Examples on Physical infrastructure authorities are Department for Transport, Public roads authorities and Confined areas authorities like harbour authorities.

  Examples: a national or regional road authority, a municipality responsible for public roads, or a port authority responsible for regulating the use of infrastructure within a confined logistics area.

- **Physical infrastructure operator (PIO)** is an entity that operates physical infrastructure used by automated vehicles. Examples on physical infrastructures operators are operators of confined

areas, e.g. ports, consolidation centres, terminals, and public road operators and contractors for road operation.

Examples: a public road operator such as cities, motorway operator, port or terminal operator, logistics-hub operator, warehouse-site operator, or contractor responsible for operating and maintaining physical infrastructure.

- **Remote operator (RO)** covers two sub-enterprise objects: The Remote assistant and the Remote driver. The Remote assistant aids the user of the automated vehicle when there is a situation where the Vehicle ITS system including the Automated Driving System cannot carry through the mission of the automated vehicle. The Remote driver provides remote driving services in those cases where the situation/incident cannot be solved by remote assistance. Examples on Remote operators can be vehicle manufacturers that can support their own makes and models or Trusted Third Parties (TTP) that have the required digital infrastructure and trained and certified personnel to handle any vehicle make and model. The last alternative requires a European standardised interface for remote operation ensuring safety, security and interoperability on a European level.

  Examples: a vehicle manufacturer providing remote support for its own vehicles, a logistics operator operating a fleet-control centre, or an independent certified service provider offering remote assistance or remote-driving services to several vehicle operators. Remote assistance and remote driving may be performed by different organisations and may be subject to different qualification, technical and regulatory requirements.

- **Security service provider (SSP)** is an entity that supports most of the entities with security services providing as a minimum the security measures confidentiality, integrity and availability. Within the MODI Enterprise View this role is defined in terms of digital and cyber security: it covers the protection of systems, networks, software and data against digital attack, unauthorised access and manipulation, and includes the operation of a security scheme based on European legislation and international security standards, credential and certificate management, monitoring of the security measures implemented by the other entities, and the handling of security incidents

  Examples: a provider of public-key infrastructure and digital certificates, a cybersecurity monitoring centre, an identity and access-management provider, or a company providing security services for connected vehicles and infrastructure.

- **Transport service provider (TSP)** is an entity that provides a transport service to the Transport service user. Examples on transport services in the MODI context are access to public roads, transport of goods, access to confined areas, loading/unloading of goods, customs handling, border crossings and charging of electric vehicles. Examples on Transport service providers are carriers, road and confined area operators, customs and terminal operators and charging stations operators.

  Examples: a carrier transporting goods, a terminal operator providing loading or unloading services, a road or confined-area operator providing infrastructure access, a customs-service provider, or a charging-point operator.

- **Transport service user (TSU)** is an entity that requests and uses transport services provided by a Transport service provider. The bilateral expectations between the Transport service user

and the Transport service provider are covered by the two-way expectation called transport services.

Examples: a shipper, cargo owner, consignee, freight forwarder, logistics service provider, or another organisation requesting and using a transport, terminal, infrastructure-access, customs, or charging service. The applicable Transport Service User depends on the service concerned; for example, a shipper may use a freight-transport service, while a carrier may use terminal-access or charging services.

- **Vehicle manufacturer (VM)** is an entity that designs, develops, tests, produces, and sells automated vehicles to Automated vehicle owners.

  Examples: a truck original equipment manufacturer (OEM) that designs, produces and supplies automated freight vehicles, including the integration of the automated driving system into the vehicle.

- **Societal interest representative (SIR)** is an entity that represents the interests of groups affected by automated freight transport but that do not themselves hold an operational or contractual role within the Enterprise View, including workers, other road users, local communities, consumers and other societal stakeholders (e.g. Researchers). A Societal interest representative advocates for these interests in matters such as safety, human factors, labour transition, inclusion, external communication and public acceptance. Unlike the other stakeholder groups introduced in this chapter, the Societal interest representative does not originate from the MODI Enterprise View but has been added specifically for the BoR to ensure that the interests of these affected groups are explicitly represented in the recommendation cards.

  Examples: a workers' union representing employees affected by the automation of logistics and terminal operations, or a road authority acting in its representative capacity for the interests of local communities and other road users (in addition to any Physical or Digital infrastructure authority role the same organisation may hold).

The stakeholder terminology defined in this chapter is used as the common reference framework for the recommendation cards in Chapter 5. The cards refer to the relevant entities by using the stakeholder labels and abbreviations introduced above, thereby supporting consistency across the thematic recommendation areas.

The stakeholder references are descriptive and do not assign legal obligations, implementation responsibility, contractual liability or priority. The concrete allocation of responsibilities may differ between countries, use cases and operational domains, and one legal entity may fulfil more than one role. Automated freight transport also affects groups that do not themselves hold an operational or contractual role within this architecture, including other road users, local communities, employees, professional drivers, terminal and warehouse personnel, emergency services and the general public. Where these groups are represented by an organised entity, for example a workers' union or a road authority acting in this capacity, that entity is captured under the Societal interest representative (SIR) object introduced above. Where relevant, the interests of these groups are addressed in the recommendations concerning safety, human factors, organisational change, external communication, trust and societal acceptance.

4 MODI legacy: Advancing automated freight transport in Europe

MODI investigates the deployment of SAE Level 4 automated freight transport in real logistics operations. Rather than focusing solely on vehicle technology and automation, the project examines how automated trucks interact with logistics processes, infrastructure, digital services (positioning services, etc.), regulatory frameworks and operational stakeholders across the freight transport system.

This chapter positions MODI within the wider European research and innovation landscape. It first outlines how MODI builds on previous and ongoing EU funded projects, then highlights the project's main contributions to the development of the field and finally explains how the MODI results are being taken forward into emerging EU initiatives and deployment programmes.

MODI builds on a sequence of European research and innovation projects addressing automated and connected mobility. Over the past decade, Horizon 2020 and Horizon Europe projects have progressively addressed key challenges related to automated freight transport, including vehicle automation, connectivity, digital infrastructure, logistics operations and CCAM integration in logistics, traffic management, electrification, safety assurance and evaluation methodologies. Relevant previous and parallel projects include e.g. AWARD, MAGPIE, ENSEMBLE, ORCHESTRA, HIDRIVE, ULTIMO, PODIUM, NordicWay, and FAME, each contributing knowledge in complementary domains.

Among these, the Horizon 2020 project AWARD established an important foundation by demonstrating highly automated heavy-duty vehicles in ports, terminals, airports and hub-to-hub logistics, including operation under adverse weather conditions. AWARD showed that automated freight vehicles can operate safely in controlled and semi-controlled environments while also highlighting the importance of regulation, operational procedures, business models and stakeholder acceptance for successful deployment.

MODI builds on these achievements and addresses several remaining gaps. While earlier projects primarily focused on vehicle functions, specific use cases or confined operational environments, MODI investigates how automated freight transport can be integrated into complete logistics chains spanning public roads, terminals, ports, digital services and regulatory processes. In this respect, MODI represents a progression from technology validation towards deployment-oriented research and demonstration.

4.1 MODI contributions to the European State of the Art

Demonstrating CCAM as an integrated logistics ecosystem

A key contribution of MODI is the shift from a vehicle-centred approach to a logistics-system perspective.

Previous projects have demonstrated automated vehicles or sub-systems in specific operational environments. MODI extends this work by investigating how highly automated freight vehicles interact with the wider logistics chain.

The MODI demonstrations include automated driving on public roads, automated terminal and port operations, automated loading and unloading, automated charging, digital customs procedures, gate access functions and remote supervision. This allows the project to evaluate not only vehicle performance but also how automated freight transport can be integrated into existing logistics processes and operational workflows.

The demonstrations showed that successful deployment depends on the interaction between vehicles, infrastructure, digital services, logistics operators and public authorities. As a result, the project generated knowledge that extends beyond vehicle automation and addresses the practical conditions required for commercial deployment.

Corridor-scale and cross-border validation

MODI advances the state of art by validating automated freight transport at corridor level across multiple countries and operational contexts.

The Rotterdam-Oslo corridor combines ports, terminals, motorways, urban roads and an international border crossing within a single logistics chain. This provides practical experience with issues that are central to future European deployment, including permitting across jurisdictions, digital customs procedures, connectivity continuity, roaming between network operators and the allocation of operational responsibilities across borders.

The project provides one of the first comprehensive evidence bases for cross-border automated freight transport in Europe.

This corridor-level experience is directly relevant to the European initiative on large-scale cross-border testbeds for connected and automated mobility, in which automated freight transport is one of the priority application domains [7]. The corridor assessment methodology, the evidence on permitting across jurisdictions and the operational experience with connectivity continuity and digital customs procedures developed in MODI provide transferable input for the design, preparation and operation of such testbeds.

Expanding readiness beyond vehicle technology

MODI extends the concept of deployment readiness beyond vehicle performance.

MODI has demonstrated that vehicle capability alone is insufficient as a measure of readiness for large-scale deployment. Successful operation depends equally on the availability and quality of infrastructure, positioning services, digital systems, connectivity, logistics processes and regulatory frameworks.

To assess these factors, MODI developed and applied a corridor-level readiness assessment covering physical and digital infrastructure along the Rotterdam-Oslo corridor. The assessment addressed road infrastructure, lane markings and signage, high-accuracy positioning services, HD mapping, mobile network coverage, charging infrastructure, safe stopping opportunities and operational constraints.

The results show that readiness for automated freight transport cannot be treated as a binary condition. Instead, readiness varies across infrastructure segments and depends on the combined availability and robustness of multiple supporting systems. The findings also underline the importance of interoperability, data availability, regulatory alignment and coordination between public and private stakeholders.

Evidence for European deployment

MODI provides practical evidence on the conditions required for deployment of automated freight transport in Europe, by studying how automated operations interact with logistics processes, infrastructure, business requirements and regulatory conditions in real operational environments.

By combining technical demonstrations with assessments of infrastructure readiness, logistics operations, business models, societal impacts and stakeholder perspectives, MODI provides strategic insights and decision support for infrastructure managers, road authorities, logistics operators, technology providers and policymakers.

The project therefore contributes not only to advances in automated driving technology, but also to the broader knowledge base needed to support and prepare for future deployment of automated freight transport at scale.

4.2 Supporting Europe's next generation of CCAM initiatives

The knowledge and recommendations developed through MODI provide a foundation for the next generation of European CCAM initiatives. By addressing deployment challenges related to infrastructure readiness, digital ecosystems, logistics integration, regulation and stakeholder collaboration, the project provides insights that accelerate the transition from research and demonstration towards large-scale deployment of highly automated freight transport.

The outcomes of MODI directly support the objectives of the CCAM Partnership [5] by providing deployment-oriented evidence from real freight transport operations. In particular, the project contributes knowledge on corridor operations, cross-border transport, logistics integration and infrastructure readiness that complements the broader CCAM research portfolio.

The project's findings and recommendations are already providing input to several ongoing and emerging European initiatives, including:

- **Large-scale CCAM demonstration programmes**, by validated freight use cases, methodologies for corridor and infrastructure readiness assessment, and practical experience from multi-country demonstrations, remote-supervision concepts, regulatory coordination and cross-border operations.
- **The European Connected and Autonomous Vehicle Alliance (ECAVA**) [6], by practical experience on interoperability between vehicles, infrastructure and logistics systems, data governance, digital infrastructure and cross-sector collaboration required for large-scale deployment.
- **The EU large-scale cross-border testbeds for connected and automated mobility** [7], by providing a validated corridor methodology, evidence from multi-country freight demonstrations, and practical experience with cross-border permitting, connectivity continuity, remote supervision and digital customs procedures. The testbeds in turn feed evidence on deployment progress and remaining barriers into ECAVA and into the wider European roadmap for automated mobility.
- **Future industrial roadmaps, standardisation activities and policy initiatives,** by identifying remaining technological, operational and regulatory barriers while providing evidence-based recommendations that support safe, interoperable and commercially viable deployment of automated freight transport across Europe.

The project outcomes are also relevant to the preparation of the Strategic Research, Innovation and Deployment Agenda (SRIDA) for the period 2028–2034, which is being developed to provide strategic advice on the research and innovation priorities supporting the competitiveness, sustainability and resilience of the European automotive sector [41]. This agenda is expected to inform the next European Framework Programme and the European Competitiveness Fund, building on current initiatives including the CCAM Partnership, the cross-border testbeds and ECAVA. MODI contributes deployment-oriented evidence on corridor readiness, cross-border operation, logistics integration and the regulatory conditions for automated freight, which addresses several of the deployment-related priorities that such an agenda is intended to cover.

Together, these contributions ensure that the knowledge generated in MODI extends beyond the project itself, supporting future European research, deployment activities and policy development, and strengthening Europe's pathway towards scalable and interoperable automated freight transport.

4.2.1 Lessons learned from MODI deployment activities

The MODI project generates evidence on the deployment conditions for SAE Level 4 automated freight transport in logistics operations across public roads, confined areas and national borders. The lessons learned presented in this chapter synthesise findings from stakeholder requirements, infrastructure analyses, system architecture work and use case demonstrations. They are intended to identify recurring findings across deliverables rather than to formulate additional recommendations.

Automated freight deployment requires system-level integration

A central lesson from MODI is that SAE Level 4 automated freight transport cannot be treated as an isolated vehicle function. The stakeholder requirements collected in D1.1 show that logistics actors, technology providers and road authorities expect automated trucks to be integrated into existing logistics processes, digital management systems, terminal operations, infrastructure services and regulatory procedures. Benefits such as higher vehicle utilisation, reduced dependency on human drivers and improved operational predictability can only be realised if the automated vehicle is embedded in the wider transport and logistics system. [42], [45]

This finding was confirmed by the use cases, in which automated driving was combined with gate access, loading and unloading, charging, customs processes, remote support, connectivity services and traffic-management functions. MODI therefore shows that deployment readiness depends not only on the maturity of the Automated Driving System, but also on the readiness of surrounding operational, digital and organisational interfaces. [56] [57] [58] [59]

Physical infrastructure should be improved selectively rather than redesigned comprehensively

The infrastructure analyses indicate that large-scale reconstruction of existing road infrastructure is neither realistic nor necessary as the primary pathway towards automated freight deployment. Current road infrastructure can support automated driving in many conditions, provided that specific readiness issues are addressed. These include lane marking quality, signage consistency, road-surface maintenance, safe stopping options, special infrastructure sections and interfaces between public roads and confined logistics areas. [52] [59]

MODI therefore supports a targeted infrastructure approach. Physical adaptations should be prioritised where they remove concrete operational barriers, such as missing safe-haven areas for Minimal Risk Manoeuvres, insufficient visibility of lane markings, complex gate environments, tunnels, bridges, border crossings or transitions between motorway and urban environments. The project evidence suggests that such measures are more feasible and proportionate than network-wide physical upgrades. [52] [53] [59]

Digital infrastructure is a core deployment condition

While physical infrastructure remains important, MODI demonstrates that digital infrastructure is a decisive enabler for scaling automated freight operations. Reliable connectivity, C-ITS services, high-accuracy positioning, HD maps, machine-interpretable traffic regulations and real-time road-event data are required to support automated vehicles beyond controlled or site-specific environments. [52] [54] [59]

The corridor assessment showed that readiness must be evaluated at segment level rather than assumed for an entire route. Connectivity, GNSS/RTK availability, map quality, traffic-event data, charging availability and safe-stopping options vary across the corridor and directly affect the feasible Operational Design Domain. This confirms that digital infrastructure should be treated as an operational layer of automated freight deployment, not as an optional support service. [59]

Cross-border deployment exposes regulatory and procedural fragmentation

The Norwegian use case showed that cross-border automated freight operation is technically feasible, but that it remains dependent on coordinated permit processes, aligned documentation, clear allocation of operational responsibilities and reliable handover between national systems. The preparation of cross-border trials required iterative dialogue with authorities and highlighted differences in national approval procedures, safety-case expectations and operational requirements. [58]

This lesson is relevant beyond the individual use case. Automated freight corridors will require harmonised or mutually compatible approaches to permits, remote operation, digital customs, connectivity handover, geodetic reference frames, incident procedures and traffic regulations. Without such alignment, deployment may remain limited to national or site-specific operations, even where the vehicle technology itself is sufficiently mature. [58] [59]

Confined areas are suitable early deployment environments, but still require standardised interfaces

Ports, terminals, yards and other confined logistics areas provide favourable conditions for early deployment because access can be controlled, traffic environments are more predictable and local operating rules can be defined by the site operator. MODI nevertheless shows that these environments are not automatically ready for unmanned operation. Gate access, yard routing, loading and unloading, charging, trailer handling and precise positioning need to be supported by digital processes and standardised interfaces. [53] [57]

The Swedish use case demonstrated the relevance of end-to-end logistics integration, including automated loading and unloading, charging, gate access and interaction with logistics management processes. This confirms that confined-area readiness is not limited to the driving task but includes the ability of the vehicle to participate in operational workflows that are currently often handled by human drivers or terminal staff. [57]

Remote operation and human factors remain essential deployment topics

MODI confirms that remote operation, remote assistance and human-system interaction are central elements of Level 4 freight deployment. Even where the vehicle performs the dynamic driving task automatically within its ODD, human operators may still be required for supervision, exception handling, recovery, communication with authorities, cargo-related decisions or operational replanning. [46] [58]

Human factors therefore need to be addressed early in system design. MODI findings point to the importance of operator situational awareness, workload management, fatigue prevention, clear alert prioritisation, robust HMI design and defined procedures for intervention. The feasibility of scalable remote supervision depends not only on communication technology, but also on safe operational concepts, certification, training and clear responsibility allocation. [46] [58]

Standardisation is required to avoid fragmented deployment

Across the MODI deliverables, standardisation emerges as a recurring condition for scalable deployment. Relevant areas include Vehicle-to-Everything (V2X) and C-ITS communication, HD map formats, geodetic reference frames, machine-interpretable traffic regulations, remote-operation interfaces, terminal processes, charging interfaces, logistics-system APIs, Public Key Infrastructure (PKI) and cybersecurity frameworks. [54] [59]

The project evidence indicates that proprietary or site-specific solutions may support individual demonstrations, but they are unlikely to enable interoperable corridor-scale operation. Automated freight deployment therefore requires interfaces and data models that work across OEMs, infrastructure operators, digital service providers, logistics actors and national jurisdictions. [53] [54] [59]

Business value depends on operational redesign, not vehicle automation alone

The stakeholder requirements show that logistics actors expect automated freight to contribute to cost reduction, capacity gains, higher reliability, improved working conditions and potentially 24/7 operations. However, these benefits depend on the ability to redesign operational processes around automated vehicles. This includes fleet planning, terminal processes, charging strategies, remote support, maintenance, customer interaction and integration with logistics management systems. [42]

MODI findings suggest that business models for automated freight should be developed at logistics-system level [45]. The value proposition is not created solely by replacing the driver in the vehicle, but by combining automated driving with digitalised logistics processes, predictable operations, standardised interfaces and new forms of cooperation between transport providers, infrastructure operators and technology suppliers. [42][45][57] [59]

Deployment should proceed through phased and evidence-based expansion of the ODD

A further lesson is that automated freight deployment should be approached as a gradual expansion of operational capability. MODI findings support starting with high-volume, predictable and well-characterised routes or confined areas, before moving towards more complex mixed-traffic, cross-border and corridor-scale operations. [42] [59]

The ODD should not be treated as a binary property of whether a route is suitable or unsuitable. Instead, it should be defined and assessed in relation to specific route segments, infrastructure conditions, connectivity availability, positioning quality, traffic complexity, weather exposure, fallback

options and operational procedures. This segment-based understanding is particularly important for long-distance freight corridors. [59]

Lessons learned for future deployment activities

Overall, MODI demonstrates that automated freight deployment requires coordinated progress across vehicle technology, infrastructure, digital services, logistics operations, regulation and stakeholder governance. The project confirms the technical feasibility of several key functions, while also showing that scalable deployment depends on harmonised interfaces, clear responsibilities, targeted infrastructure readiness, robust digital services and evidence-based approval procedures. [56] [57] [58] [59]

Future deployment activities should therefore combine technical validation with operational and institutional preparation. This includes early involvement of authorities and infrastructure operators, structured safety cases, harmonised permit documentation, realistic logistics integration, long-term field testing and continuous feedback from users and stakeholders. These elements are necessary to move from demonstration-level feasibility towards repeatable, transferable and scalable automated freight operations. [42] [58] [59]

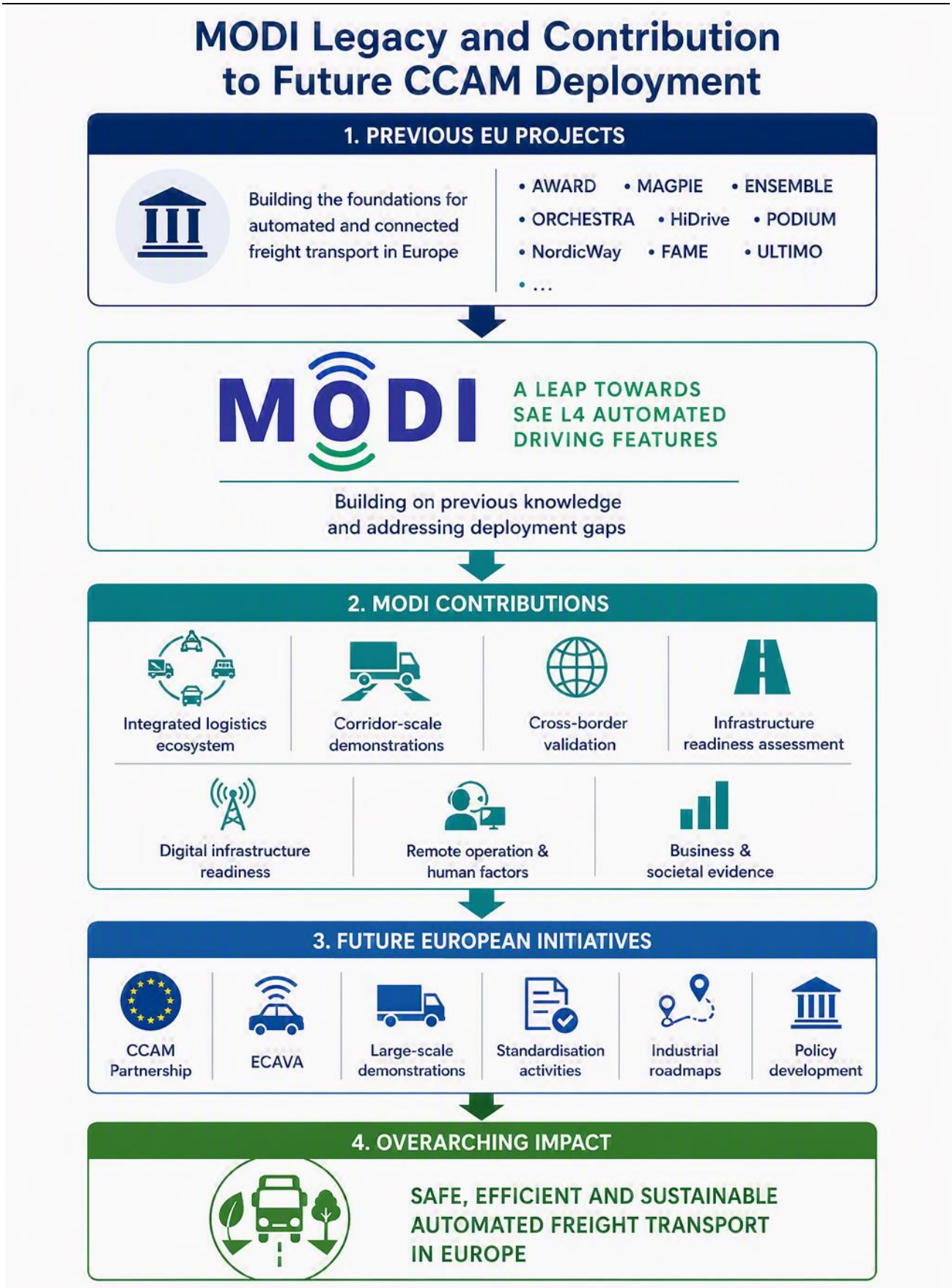


Figure 5: MODI's contribution to future European deployment of automated freight transport

5 Recommendations

This chapter presents the consolidated 90 recommendations derived from the MODI project. The recommendations describe what should exist for successful deployment of SAE Level 4 CCAM freight operations (physical and digital infrastructure); how it should be operated (logistics and operational aspects); and how it should be governed to enable deployment at scale (standardization and regulation). In other words, they are structured in five thematic areas in the following order:

- **Physical infrastructure** – addresses the assets and environments in which automated vehicles operate.
- **Digital infrastructure** – needed to enable communication, coordination and information exchange across vehicles, infrastructure and logistics actors.
- **SAE Level 4 integration in logistics** – addresses how these capabilities can be integrated progressively into logistics processes and business operations.
- **Standardisation** – provides the common interfaces needed for interoperability across technologies and organisations
- **Regulation** – establishes the legal and institutional framework within which deployment can occur.

Within each of these thematic areas, recommendations are further grouped into recommendation cards that identify the relevant stakeholder groups, the main challenges addressed, the recommended actions, and an indicative deployment horizon. Each recommendation card is assigned a unique alphanumeric identifier (e.g., RC-PI-1) in which the letter code denotes the thematic area (e.g., PI = Physical Infrastructure) and the number indicates the card's position within that area. The full wording and traceability of all consolidated recommendations are provided in Annex I.

The chapter should be read as a synthesis of project evidence and stakeholder input rather than as a prescriptive implementation plan. Concrete responsibilities, priorities and timelines may differ depending on the operational context, national framework and maturity of the respective deployment environment.

5.1 Physical Infrastructure

Physical infrastructure forms the operational environment in which SAE Level 4 CCAM freight vehicles perceive, plan and execute their driving tasks. In MODI, this includes not only public road corridors and infrastructure, but also ports, terminals, yards, gates, loading areas, charging facilities and transitions between public and confined areas. The physical infrastructure challenge is therefore not limited to road design. It also concerns the continuity of automated freight operations across logistics nodes, industrial areas and cross-border transport corridors.

Physical infrastructure requirements depend strongly on the ODD, the degree of mixed traffic, the level of infrastructure control and the type of logistics operation. Confined areas such as ports and terminals may provide more controlled conditions for early deployment – that is, environments where key operational variables can be managed or restricted, for example operations within a geographically restricted site with predefined routes, lower speed limits and limited access for the general public, but they still involve interactions with manually operated vehicles, terminal staff, access-control processes, loading operations and site-specific traffic rules. Public-road sections introduce additional variability, including different road authorities, road layouts, signage practices,

traffic conditions and special infrastructure sections such as tunnels, bridges, borders or motorway–urban transitions.

For this reason, the physical infrastructure recommendations in MODI should be understood as a set of targeted readiness measures rather than as a call for uniform, large-scale reconstruction of the road network.

The recommendations point towards clear, consistent and well-maintained infrastructure, selective support at safety-critical points, driverless readiness of logistics sites and better alignment between public-road and confined-area environments.

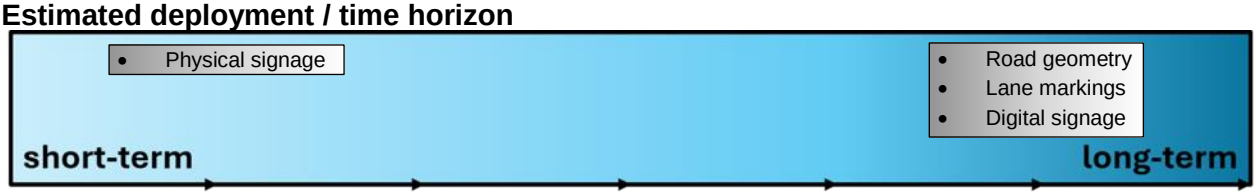
RC-PI-1	Physical Infrastructure Readiness and Legibility												
Stakeholder	AVO	AVU	**CB**	DIA	**DSP**	**PIA**	**PIO**	RO	SSP	**TSP**	TSU	VH	SIP
Main Challenges Addressed: • Variability of physical infrastructure conditions across public road corridors, ports, terminals and logistics hubs • Inconsistent/ambiguous/complex lane markings, signage, road-surface quality and layout characteristics • Need for infrastructure that can be interpreted consistently by automated vehicles and human road users Relationship between physical infrastructure quality, digital mapping and operational readability													
Recommendations • PI-01 – Establish CCAM-ready infrastructure criteria for corridors, ports, terminals and logistics hubs, covering road geometry, lane markings, signage, maintenance, connectivity readiness and operational access conditions. • PI-02 – Keep road and terminal layouts simple, consistent and machine-interpretable; avoid infrastructure designs that are overly complex or tailored to a single technology provider. PI-04 – Define higher maintenance and visibility standards for lane markings, signage and road surface quality to support automated freight operations.													
Estimated deployment / time horizon 													

Figure 6: Recommendation Card: Physical Infrastructure Readiness and Legibility

Need for harmonisation

The deployment of SAE Level 4 CCAM freight vehicles depends on physical infrastructure that is consistently interpretable across corridors, ports, terminals and logistics hubs. Evidence from the MODI project highlights significant variability in infrastructure conditions along the corridor, including differences in lane markings, signage, road-surface quality and layout characteristics [59]. Such inconsistencies create operational uncertainty for automated vehicles and complicate the definition of stable operational design domains, particularly at interfaces between public roads and confined logistics areas [52] [53] [59]. Establishing harmonised CCAM-ready infrastructure criteria is therefore essential to provide a common reference framework for infrastructure readiness across different countries, operators and use cases. The criteria should be developed through a joint process

involving the stakeholders listed in Chapter 3. Their selection should be based on evidence from multiple SAE Level 4 solutions and relevant deployment environments rather than on the capabilities or limitations of a single system.

Infrastructure vs. vehicle responsibilities

Harmonised criteria should primarily address recurrent, safety-relevant and system-wide challenges that cannot reasonably be mitigated by vehicle design alone and for which infrastructure intervention provides proportionate benefits. Limitations resulting mainly from immature or solution-specific design choices should, in principle, be addressed by the vehicle or automated driving system (ADS) provider rather than translated directly into infrastructure requirements. The assessment should also consider the effects of L4 system behaviour on mixed traffic, including predictability, interaction with other road users and public acceptance. Where operational problems are primarily caused by immature or inappropriate system design, improving the vehicle or ADS should be considered before investing in infrastructure adaptations. [52]

Legibility and technology neutrality

A key requirement emerging from these findings is the need for infrastructure that is legible for both automated vehicles and human road users. Simple, consistent and machine-interpretable road and terminal layouts reduce ambiguity in perception and support predictable system behaviour in mixed-traffic and logistics environments. In contrast, complex or highly customised infrastructure designs, particularly those tailored to specific technologies, may limit interoperability and increase the risk of misinterpretation by the ADS. Technology-neutral design principles are therefore necessary to ensure compatibility with multiple vehicle concepts and digital services, while maintaining usability for conventional traffic participants. [52] [53] [54]

Quality and maintenance standards

Infrastructure quality and maintenance play a critical role in supporting automated driving functions. Lane markings, traffic lights and signs and road-surface conditions directly affect perception, localisation and trajectory planning. Their degradation can significantly reduce operational readability, even where the overall infrastructure layout is suitable for automated driving. MODI findings indicate that higher and more explicit standards for maintenance and visibility are required to ensure reliable performance under varying environmental conditions, including different lighting, weather and traffic scenarios. [52] [59]

Integrating physical and digital infrastructure

At the same time, physical and digital infrastructure should be considered in an integrated manner. Reliable digital representations, such as HD maps, lane-level road networks and machine-readable traffic regulations, depend on an accurate and stable physical environment. However, digital systems alone cannot compensate for unclear or poorly maintained physical infrastructure. A balanced approach is therefore needed, in which physical infrastructure provides a clear and stable baseline for automated perception, while digital infrastructure complements this with dynamic, context-specific information on traffic conditions, restrictions and operational access.

RC-PI-2	Cost-Effective and Staged Infrastructure Investment												
Stakeholder	***AVO***	*AVU*	*CB*	*DIA*	*DSP*	***PIA***	***PIO***	*RO*	*SSP*	***TSP***	*TSU*	***VM***	*SIR*

Main Challenges Addressed:

- Heavy-vehicle charging network not yet mature, and physical charging not yet automated

Risk of unrealistic or non-cost-effective large-scale infrastructure upgrades

Recommendations

- PI-08 — Prepare charging infrastructure for automated freight vehicles in two steps: first ensure a sufficiently mature heavy-vehicle charging network, then enable physical automation of charging (vehicle positioning, access space, connector handling and scalability for fleets).
- PI-11 — Prioritise targeted, scalable and high-impact infrastructure measures, and avoid large-scale physical upgrades where these are not operationally realistic or cost-effective.

Estimated deployment / time horizon

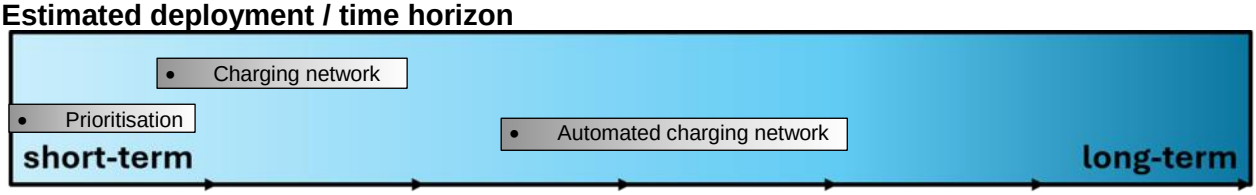


Figure 7: Recommendation Card: Cost-Effective and Staged Infrastructure Investment

Strategic principle for infrastructure investment

The infrastructure requirements identified across the cards in this chapter collectively imply a substantial investment agenda. The two recommendations bundled in this card establish the strategic principle that governs how such investment should be approached:

- charging infrastructure, identified as a structurally distinct and economically significant requirement, should be developed in two stages: first by ensuring sufficient network coverage and capacity for heavy-duty vehicle charging, and subsequently by enabling the physical and digital automation of the charging process, while…
- infrastructure investment in general should prioritise targeted, scalable interventions over comprehensive physical upgrades.

Charging network maturity as the priority

For heavy-duty electric freight vehicles, charging availability constitutes a mission-critical operational constraint, thus establishing a sufficiently mature charging network before addressing the physical automation of the charging process itself should have one of the highest priorities.

Corridor-level energy consumption modelling indicates that a heavy-duty vehicle operating with a typical payload would require multiple charging stops to traverse the full corridor, reinforcing simultaneous-demand considerations [59]. On this basis, the recommended sequencing – first ensuring network maturity through site audits, capacity planning, and targeted incentives for truck-capable charging locations along the network, and only subsequently addressing automation of the charging process itself – reflects the empirical finding that network coverage, while currently adequate at the level of individual vehicles, has not yet been validated for fleet-scale operation [59].

The second stage of charging readiness

The second stage of charging readiness concerns the physical and digital automation of the charging interaction itself, rather than the spatial coverage of charging sites. Project requirements for autonomous charging identify a chain of functions that must be handled without driver presence:

- charging must be planned and confirmed digitally,
- a suitable charging slot or charging point must be allocated,
- the vehicle must be able to position itself at the charger, and
- the charging process must provide status and exception information to the relevant operational interface [46] [48].

These requirements connect physical infrastructure design directly to communication and HMI design: access space, docking precision and connector handling are only operationally useful if the vehicle, charging infrastructure and remote or fleet-side interface can exchange the information needed to initiate, monitor, interrupt or recover the charging process [46] [48]. The evidence therefore supports treating automated charging as a later-stage capability that depends on prior network maturity, standardised charging interfaces and operational feedback processes, rather than as the first prerequisite for SAE Level 4 freight deployment [46] [48] [59].

Targeted, scalable interventions

The principle of prioritising targeted, scalable interventions over large-scale physical upgrades reflects a consistent finding across the project's infrastructure assessment work.

Investigation into the physical infrastructure requirements for automated freight on public roads concluded that

- current infrastructure is largely sufficient for automated vehicles,
- that manufacturers are designing systems to operate within the existing road network rather than requiring dedicated infrastructure such as CAV-only lanes, and
- that major CAV-specific infrastructure upgrades would be prohibitively costly relative to their operational benefit [52].

The expectation arising from this assessment is that physical infrastructure will remain largely unchanged, with future development effort concentrated on digital infrastructure, which offers greater flexibility in adapting to the evolving needs of automated transport [52]. The corridor-wide assessment reinforces this orientation from a different angle, recommending that – given budget constraints affecting road authorities – a prioritised list of "no-regret" measures should be established, beginning with those interventions that combine high operational impact with low investment risk, accompanied by short-, medium- and long-term cost estimates to support decision-making [59].

Taken together, these findings position infrastructure investment for SAE Level 4 freight transport as a disciplined, evidence-based selection of high-value interventions. Charging infrastructure illustrates this logic particularly clearly: basic network availability and fleet-scale capacity should be addressed before the more specialised automation of the charging act itself can create operational value [59]. The same sequencing principle applies across the wider physical infrastructure agenda, where safe-haven areas, infrastructure-based sensing, special-section measures and confined-area digitalisation should be prioritised where they remove concrete operational barriers and can be

scaled across comparable sites or corridor sections [52] [59]. This approach preserves investment realism while still enabling progressive readiness for automated freight operations.

RC-PI-3	Safety-Critical Support, Fallback and Special Sections												
Stakeholder	*AVO*	*AVU*	*CB*	*DIA*	*DSP*	*PIA*	*PIO*	*RO*	*SSP*	*TSP*	*TSU*	*VM*	*SIR*

Main Challenges Addressed:

- No designated safe-haven or fallback locations for Minimal Risk Manoeuvres and recovery
- Safety-critical points (gates, VRU conflict zones, intersections, loading areas) lacking infrastructure-based support
- Special sections (tunnels, bridges, tolling, borders, motorway–urban transitions) needing dedicated readiness measures

Recommendations

- PI-03 — Provide safe-haven areas and physical fallback locations for Minimal Risk Manoeuvres, recovery operations and controlled stops along corridors and inside logistics hubs.
- PI-05 — Deploy infrastructure-based sensing selectively at safety-critical points such as ports, gates, vulnerable road user conflict zones, intersections, loading areas and confined areas.
- PI-10 — Address special infrastructure sections such as tunnels, bridges, tolling points, borders and motorway–urban transitions with dedicated automation-readiness measures.

Estimated deployment / time horizon

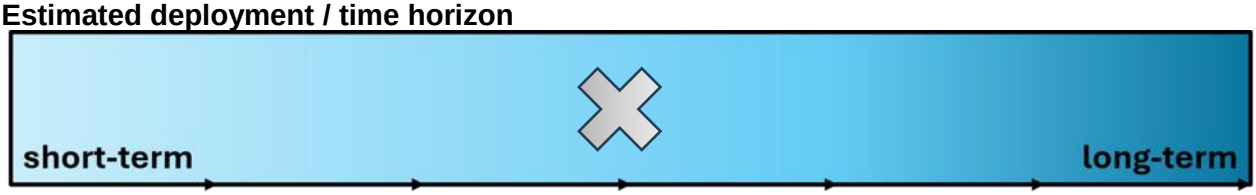


Figure 8: Recommendation Card: Safety-Critical Support, Fallback and Special Sections

Corridor-wide baseline requirements

The physical infrastructure requirements for SAE Level 4 automated freight are not uniform across the network. A distinction should be made between corridor-wide baseline requirements and targeted measures for specific locations. Baseline requirements, including adequate maintenance and visibility standards for lane markings, signage and road surface quality, should apply consistently across roads intended for SAE Level 4 freight operation, as described in RC-PI-1.

Targeted measures for specific locations

Beyond these baseline measures, a distinct category of readiness concerns specific locations where standard infrastructure conditions are insufficient and targeted provisions are required to ensure that automated vehicles retain a viable path to safe stoppage, can receive anticipatory hazard information in areas of limited sensor coverage, or can navigate infrastructure geometries that impose constraints not encountered elsewhere along the route. The three recommendations in this card address this second category. They share the principle that additional physical infrastructure intervention should be selective and proportionate, concentrated at the points where the baseline provisions are insufficient and the safety consequences of inadequate provision are highest [52].

Safe stopping and recovery locations

A prerequisite for safe SAE Level 4 freight deployment on public roads is the availability of physical locations where automated vehicles can perform MRM without creating hazards for surrounding traffic. Corridor assessments along the Rotterdam – Oslo route found that approximately 64% of the 2,848 km corridor meets the minimum shoulder width threshold required for MRM compliance, with substantial national variation: Germany and the Netherlands show compliance rates above 75%, whereas Sweden falls below 46% [59]. These results indicate that sizeable contiguous stretches remain unsuitable for controlled stops – a finding with direct operational consequences for heavy-duty automated freight vehicles that require more stopping distance and lateral clearance than passenger vehicles. The challenge is compounded at structural elements such as bridges, where narrow or absent hard shoulders and the impossibility of returning to a prior position create conditions in which an MRM would itself generate safety risks [58]. Project findings confirm that no unified approach to safe-haven placement, spacing, or specification currently exists along the corridor, and that resolving this gap requires structured collaboration between vehicle operators and national road authorities [52]. Inside logistics hubs and terminal areas, the same requirement applies – designated recovery positions should be incorporated into site layouts to enable controlled restart after exception events without disrupting ongoing operations.

Selective infrastructure-based sensing

Selective deployment of infrastructure-based sensing at specific locations addresses a complementary safety aspect: improving hazard detection where interaction density and occlusion conditions exceed the reliable coverage of vehicle-mounted sensors alone. Demonstrations at a complex urban intersection on the motorway-to-harbour transition route in Use Case Germany confirmed that roadside LiDAR sensors substantially improve the detection of vulnerable road users in occluded scenarios, with infrastructure and vehicle perception exhibiting complementary strengths – elevated sensors providing persistent coverage behind parked vehicles and street furniture, while onboard systems deliver more detailed object classification in unobstructed conditions [56].

A central design principle that emerged from this work is that infrastructure-provided perception data can function as a supplementary redundancy layer rather than a binding safety-critical input: final responsibility for object classification, trajectory planning and manoeuvre execution must remain with the vehicle [56][52]. This delineation is essential both for legal clarity and for functional safety, since roadside sensors are subject to maintenance and calibration states that cannot meet the reliability guarantees applicable to certified vehicle systems. Selective deployment at gates, port entrances, vulnerable road user conflict zones and confined area interfaces is operationally effective and cost-justified; network-wide coverage is neither warranted nor technically necessary within a vehicle-centric design paradigm [52].

Special infrastructure sections

Special infrastructure sections such as tunnels, bridges, tolling points, national border crossings and motorway-to-urban transitions impose constraints that require dedicated automation-readiness treatment rather than simple extensions of the general corridor baseline:

- Tunnels introduce simultaneous GNSS outages, reduced cellular connectivity, and severely restricted MRM capability, while also requiring machine-readable provision of height, width and cargo restrictions [52] [59].

- Bridges present weight limits, wind exposure and similarly absent safe-harbour availability; at border crossings, the concurrent transition in regulatory environment, positioning reference frame and cellular operator compounds the operational challenge [52] [58].
- Corridor assessments recommend that at complex nodes the ODD should either be formally closed or vehicle functionality reduced, with pre-defined and tested fallback processes documented before deployment [59].

This selective, safety-driven logic complements the corridor-wide baseline requirements described in RC-PI-1. While adequate maintenance, visibility and road-surface standards remain relevant across roads intended for SAE Level 4 freight operation, large-scale physical transformation of public road infrastructure is neither economically realistic nor operationally necessary. Additional infrastructure measures should therefore be targeted at locations where the risk profile exceeds what vehicle systems can reasonably manage under the defined baseline conditions.

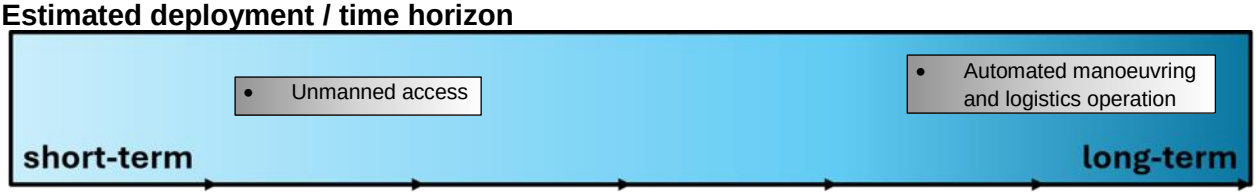
RC-PI-4	**Confined Areas and Logistics-Site Readiness**												
Stakeholder	***AVO***	***AVU***	*CB*	*DIA*	*DSP*	***PIA***	***PIO***	*RO*	*SSP*	***TSP***	***TSU***	***VM***	*SIR*
Main Challenges Addressed: • Physical access to ports, terminals, gates and yards not enabled for unmanned operation • Inconsistent dock, ramp and loading geometry for precise automated manoeuvring • No designated automation-ready zones for early, controlled deployment • Operational discontinuities between public roads and confined areas													
Recommendations • PI-06 — Enable unmanned physical access to ports, terminals, gates, yards and loading docks, including automated entry, loading and unloading procedures. PI-07 — Once harmonised standards are available (e.g. on digital goal posts), implement them consistent in dock, ramp, loading, unloading and trailer-handling geometry so that automated vehicles can perform precise manoeuvring and logistics operations reliably. • PI-09 — Designate automation-ready zones in industrial areas, ports, terminals and logistics sites to enable early deployment under controlled but scalable conditions. • PI-12 — Aim for alignment between public-road and confined-area infrastructure requirements to avoid operational discontinuities between public roads, ports, yards and terminals.												
Estimated deployment / time horizon 													

Figure 9: Recommendation Card: Confined Areas and Logistics-Site Readiness

Scope and relationship to baseline requirements

This card complements the baseline readiness requirements defined in RC-PI-1. Whereas RC-PI-1 addresses consistent physical-infrastructure conditions across public roads and confined areas, RC-PI-4 focuses on the additional site-specific provisions required for the transition into and operation within confined logistics areas, including gate access, manoeuvring, docking and interaction with loading and unloading facilities.

Confined sites as integrated deployment environment

Confined logistics sites represent both a primary near-term deployment environment for SAE Level 4 freight vehicles and an operational context that differs structurally from public roads. These areas are privately operated, are typically not publicly accessible, and the responsible site operator functions as a local counterpart to a road authority, governing local operational safety and traffic flow without assuming responsibility for the automated vehicle's own functional safety [53]. Because SAE Level 4 vehicles need operate seamlessly across both public roads and confined sites within a single mission, readiness in this domain cannot be addressed in isolation from the broader corridor; the four recommendations in this card jointly define what site-level readiness entails and how it connects to the wider physical infrastructure baseline.

Driverless access and precise positioning

Enabling driverless physical access to confined sites requires that the full set of interactions traditionally performed by a driver such as gate registration, route assignment within the site, and precise positioning at docks or loading bays be digitalised end to end. Project work has conceptualised this transition through a "valet parking" model, in which an arriving vehicle exchanges its arrival confirmation and visits identifier with a yard operating system, which in turn assumes responsibility for in-site routing and returns control to the fleet system upon departure [53]. Demonstrations of this approach within MODI confirmed its technical viability and identified the same governing principle: granting access alone is insufficient, since the vehicle also requires precise digital routing and positioning information once inside the gate, and a unified communication standard is necessary to avoid facility-specific integrations for each operator [57].

Precise dock, ramp and loading geometry is the second structural requirement, since the utility of an automated vehicle at a confined site depends on its ability to participate in loading and unloading, not merely to navigate to a location. Project findings indicate that current loading dock designs and guidelines do not require fundamental redesign, since the steering and sensing accuracy of automated vehicles is sufficient for existing dock geometries; what is required instead is the digital instrumentation of these locations through goal points and anchor points embedded in HD maps, which specify not only the destination but the precise final position and orientation needed for processes such as docking, trailer coupling, charging or cargo transfer [53].

Automation-ready zones for early deployment

The designation of automation-ready zones – controlled environments in industrial areas, ports, terminals and logistics sites that allow phased deployment under conditions narrower than full corridor operation – represents an enabling mechanism for early-stage deployment that has been identified as a priority by project stakeholders, though the available project evidence does not yet define a complete zone typology or a harmonised design specification for such areas. The more concrete evidence supports a narrower interpretation: early deployment areas should be selected and bounded through site-specific assessment of:

- route characteristics,
- traffic conditions,
- infrastructure readiness,
- ODD constraints,
- risk mitigation and approval by the relevant site or road authority.

The suitability of an area for early deployment should not be inferred solely from its categorisation as a port, terminal, yard or other confined environment [46] [47].

Controlled access concepts, such as dedicated express lanes, Automatic Number Plate Recognition (ANPR)-based access control and signal-controlled clearance processes, demonstrate how access by automated vehicles can be managed within bounded and authority-controlled environments. These concepts provide evidence that controlled operational access can support deployment, but they should not be interpreted as a generic model for determining whether a particular area is suitable for automated vehicle operation [46].

Confined sites are nevertheless well suited to this role precisely because:

- access is controlled,
- traffic composition is known, and
- the site operator can define local operating conditions,

This has already been demonstrated at the Dutch port terminal where automated vehicles operate within a single, geographically bounded and digitally instrumented environment under a dedicated terminal control centre [53] [54]

Alignment between confined areas and public roads

Alignment between confined-area and public-road infrastructure requirements addresses the operational discontinuity that arises at the interface between the two domains.

Project architecture work establishes that, from a high-level functional perspective, traffic management on confined sites and on public roads differs little, with the confined-area operator functioning as a private-terrain counterpart to a public traffic orchestrator, albeit with more limited scope, vehicle volume and geographical extent [54].

Because SAE Level 4 vehicles transition between these domains within a single mission, requirements developed for public roads (e.g. standardised C-ITS messaging, digital map formats, and positioning references) should be applied in confined areas wherever feasible rather than developing parallel, site-specific solutions, an approach already adopted for gate access through reuse of public-road C-ITS message types [53] [57].

Closing this gap requires harmonising road geometry, traffic rules, routing instruction formats, map references and access-control logic between confined and public contexts so that automated vehicles can interpret the transition between the two environments consistently and without discrepancy [53] [54]. The evidence therefore supports a staged but integrated readiness approach:

1. Enable secure and standardised unmanned access;
2. instrument docks, loading bays and yard destinations with precise digital target positions;
3. use controlled, authority-approved zones for early deployment where the operational conditions are narrower and better known; and
4. avoid divergence between public-road and confined-area infrastructure standards wherever the same vehicle mission spans both domains [46] [53] [54] [57].

5.2 Digital Infrastructure

The safe and scalable deployment of SAE Level 4 automated freight along a multi-country corridor depends not only on the physical road environment but equally on the digital infrastructure that

supports, supplements and, in certain contexts, compensates for the limitations of that physical environment. Where physical infrastructure improvements are technically complex, economically disproportionate or simply unavailable within the operational timeframes relevant to early SAE Level 4 deployment, digital infrastructure services can provide the redundancy, contextual information and operational connectivity that automated vehicles require. This trade-off – between what physical infrastructure can reliably deliver to onboard vehicle perception and what must be provided digitally – is a central design question for corridor-level automated freight and runs through each of the recommendation clusters in this chapter.

5.2.1 Connectivity and Cooperative Services

Cooperative Intelligent Transport Systems (C-ITS) provide the communication and data layer through which infrastructure and vehicles exchange safety-critical and operationally relevant information in real time. Within the existing European C-ITS frameworks, real-time information services have undergone significant definition and standardization. Based on these standards platforms and alliances such as C-Roads [9] and C2C-CC [10] developed harmonized C-ITS services and detailed specifications, which are freely available. For SAE Level 4 automated freight, cooperative services and robust connectivity encompass a range of additional layers that extend beyond what onboard vehicle perception alone can reliably provide: networks, machine-readable traffic rules and dynamic event data, remote operations etc.

The recommendations in this section address the standardisation, harmonisation, governance frameworks and deployment requirements that must be in place for these services to function coherently and interoperable across road freight corridors in Europe.

The terms used in this deliverable to describe vehicle connectivity are applied as follows:

> V2X denotes the class of communication in which a vehicle exchanges data with other vehicles, with roadside and other infrastructure, with back-end systems and, where relevant, with other road users, irrespective of the underlying radio technology. Two access technologies are currently available for V2X communication: ITS-G5, based on IEEE 802.11p, and cellular V2X (C-V2X), specified by 3GPP.
>
> Cooperative Intelligent Transport Systems (C-ITS) denote the standardised service layer carried over these access technologies, comprising the harmonised service definitions, message sets and security and certificate framework specified at European level. V2X therefore describes the communication capability, while C-ITS describes the standardised services built upon it. Where this deliverable refers to mobile networks, it denotes public cellular connectivity used for communication with back-end systems (for example remote operation, fleet and transport management, and the delivery of map and positioning correction data) as distinct from direct short-range V2X communication.

RC-DI-1	Connectivity and Communication Continuity												
Stakeholder	AVO	AVU	CB	**DIA**	**DSP**	PIA	PIO	**RO**	**SSP**	TSP	TSU	**VM**	SIR

Main Challenges Addressed:

- Maintaining reliable, safety-critical connectivity along corridors and across borders
- Seamless handover between networks, correction services and national systems during cross-border operation
- Avoiding dependence on a single communication technology
- Treating public and private communication assets (mobile, C-ITS) as core enablers rather than optional add-ons

Recommendations

- DI-01 — Ensure cybersecure, reliable and standardised connectivity – covering mobile networks, V2X communication and C-ITS services – along automated freight corridors, including interoperable inter-provider handover, network redundancy, cross-border continuity and clear responsibility for service provision, so that remote supervision and safety-critical communication remain available across different road operators and national borders as well as different communication channels and mobile network operators.
- DI-14 — Treat public digital infrastructure as a core component of transport infrastructure and apply governance, performance and investment frameworks commensurate with its role in automated freight operations.
- DI-16 — Ensure seamless handover between mobile networks, RTK correction providers, connectivity technologies and national systems during cross-border operations.
- DI-17 — Use hybrid communication architectures combining ITS-G5, C-V2X, and cellular where appropriate, rather than relying on one communication technology only.

Estimated deployment / time horizon

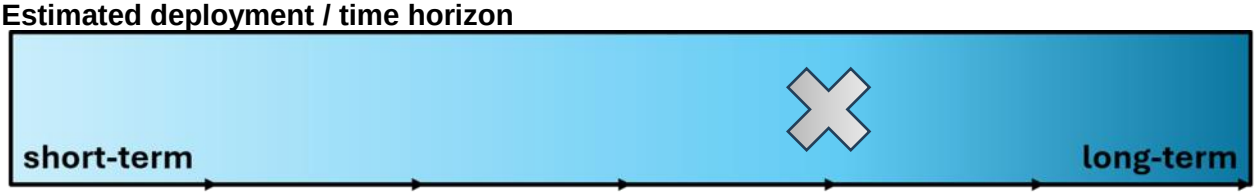


Figure 10: Recommendation Card: Connectivity and Communication Continuity

Connectivity as a cross-border operational requirement

Automated vehicles depend on connectivity for a range of safety-critical and operationally essential functions:

- remote supervision,
- data exchange with other vehicles and the infrastructure (e.g. cooperative awareness messaging, warning messaging, reception of dynamic infrastructure data,
- access to high-accuracy GNSS correction services, and
- the monitoring and logging required to support safe operation and incident handling.

Along a multi-country corridor, the challenge is not simply one of signal availability within any single communication channel, but of ensuring that these functions remain continuously available as vehicles cross road sections with different road operators and national borders, transition between infrastructure domains and interact with different mobile network operators, correction service providers and C-ITS architectures. This cross-border dimension elevates connectivity from a

technical performance parameter to a combined governance, interoperability and safety-assurance challenge. [46] [59]

Mobile-network coverage and service levels

Empirical measurements conducted along the MODI corridor provide a quantified baseline from which the recommendations in this card have been derived.

Regarding mobile networks LTE and 5G (Long Term Evolution and Fifth generation of cellular network technology) coverage was found to be broadly available, with signal loss occurring along less than two percent of the route under normal conditions. However, degradations were consistently observed near border crossings and within tunnels – precisely the infrastructure transitions that are most operationally sensitive for automated freight transport [59].

Uplink throughput, which is particularly critical for remote operation video streaming, was found to be insufficient over approximately fifteen percent of measured instances, with attainable average values of 28–33 Mbps under representative conditions [59].

Service-level requirements for SAE Level 4 freight operation further specify:

- minimum bandwidth, latency and availability thresholds, as well as
- the need for redundancy through multi-provider and multi-technology architectures.

These figures confirm that the technical baseline is promising but also demonstrate that corridor readiness cannot be assessed through average coverage statistics alone; it must be evaluated against safety-critical service levels, continuity during transitions and the availability of fallback channels.

High-accuracy positioning and supporting digital services

High-accuracy GNSS positioning – typically augmented by correction services such as Network Real-Time Kinematic (NRTK) or Precise Point Positioning-Real-Time Kinematic (PPP-RTK) – is an equally critical component of the connectivity infrastructure [52] [59].

MODI measurements demonstrated:

- NRTK availability of approximately 92% with a 95th-percentile horizontal position error of around four centimetres, while
- other correction services showed lower and more variable performance. [59]

Coverage gaps were primarily attributable to:

- tunnels,
- urban canyons and
- border crossings.

A particularly relevant finding concerns the inconsistency of national geodetic reference-frame realisations across the corridor countries, which complicates cross-border positioning continuity and reinforces the need for harmonised standards, as addressed in more detail under the positioning and mapping recommendations. After disruptions, median reconvergence times for high-accuracy services were around ten seconds – a figure that must be accounted for in fallback and degraded-mode behaviour. Beyond positioning, GNSS correction services, mobile network infrastructure, C-ITS message services, HD maps and digital access interfaces form part of the operational

environment for coordinated vehicle–infrastructure interaction, and need to therefore be harmonized, quality-monitored and made available through standardised interfaces with defined service levels. [59]

Structural gaps addressed by the recommendations

Against this background, the four recommendations bundled in this card address a set of structural gaps.

1. DI-01 establishes the overall requirement for reliable, standardised connectivity along automated freight corridors, explicitly coupling technical requirements, such as inter-provider handover or network redundancy with governance requirements, in particular clear responsibility for service provision. The MODI findings indicated multiple mobile network operators, C-ITS service providers, correction-service providers and infrastructure authority domains whose service boundaries do not align with freight logistics flows. A functional allocation of responsibilities is therefore essential, since without such allocation, there is a risk that connectivity gaps at border transitions remain unresolved.
2. DI-14 complements this framing by establishing that public digital infrastructure constitutes a core operational enabler of automated freight that must be treated accordingly in investment, governance and regulatory terms. Coverage and quality requirements for these services cannot be left to ad hoc market provision, because their performance directly affects the safety case of cross-border SAE Level 4 operations. These infrastructure components must therefore be subject to service-level requirements, availability and latency thresholds, standardised APIs, real-time data exchange protocols, integrity and plausibility checks, and continuous monitoring and logging – governance mechanisms comparable in ambition to those applied to physical road infrastructure. Planning, maintaining and quality-assuring public digital infrastructure as part of a corridor's operational readiness is accordingly a shared responsibility of multiple stakeholders.
3. DI-16 addresses the operational continuity problem at its most specific level: the seamless handover between mobile networks, RTK correction providers, communication technologies and national systems during cross-border operations. Cross-border transitions represent the highest-risk moments for connectivity loss, as vehicles may need to roam or re-authenticate with a new mobile network operator, switch correction-service providers, reconcile map and geodetic reference-frame differences, and maintain latency-sensitive links to remote supervision and safety-relevant infrastructure services. Ensuring continuity across these transitions requires multi-provider handover mechanisms, continuous connectivity monitoring and automated fallback procedures, pre-operational field testing at border sections, and harmonisation of routing and map formats across national domains. The transition at a border crossing is, in this sense, a compound process involving network roaming, GNSS correction handover, reference-frame synchronisation, and digital procedures for customs, gate access or documentation, confirming that handover is not a narrow telecommunications issue but a cross-domain continuity requirement for the entire automated freight service.
4. Finally, DI-17 addresses the communication architecture from a resilience perspective. Rather than depending on a single communication technology, automated freight vehicles should combine ITS-G5, C-V2X, and cellular where appropriate, with each medium contributing complementary capability. A hybrid architecture also strengthens fallback behaviour: safety-critical messages can be prioritised and routed across alternative channels, data can be buffered during temporary outages, and the vehicle can transition to

degraded operation, execute a Minimal Risk Manoeuvre or involve the remote operator according to predefined procedures. The interdependence of DI-01, DI-14, DI-16 and DI-17 is therefore the primary rationale for their consolidation: connectivity reliability cannot be achieved through a single technology choice or isolated policy measure, but requires the simultaneous alignment of service standards, public infrastructure commitment, cross-border handover governance, clearly allocated responsibilities and resilient multi-technology architecture design.

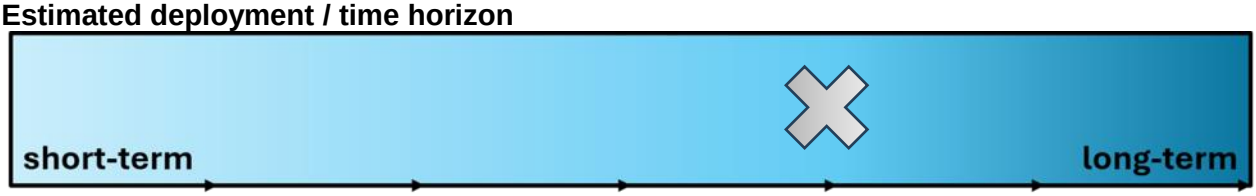
RC-DI-2	Machine-interpretable Traffic Rules and Dynamic Road Data												
Stakeholder	AVO	AVU	CB	**DIA**	**DSP**	**PIA**	**PIO**	PO	SSP	TSP	TSU	**VM**	SIR
Main Challenges Addressed: • Traffic rules and regulations not available in machine-interpretable form • Dynamic events (roadworks, closures, temporary layout changes in confined areas) not delivered in real time and machine-readable form • Heterogeneous, non-standardised infrastructure-to-vehicle information and APIs													
Recommendations • DI-02 — Provide traffic rules, restrictions and traffic regulations in digital, cybersecure machine-interpretable formats for automated vehicles. • DI-05 — Provide dynamic road, traffic and event data, such as roadworks, closures, temporary restrictions, incidents and temporary layout changes in confined areas (e.g. relocated barriers on terminals) in real time and standardised machine-interpretable form. • DI-06 — Provide standardised infrastructure-to-vehicle real-time information (e.g. signalised intersection information, variable message signs, rail crossings and lane status) together with harmonised underlying API structures, data models and service-level requirements. Ensure that digital signs, VMS feeds and temporary traffic-management information from road authorities are regulated, quality-assured and provided through reliable, standardised APIs.												
Estimated deployment / time horizon 													

Figure 11: Recommendation Card: Machine-interpretable Traffic Rules and Dynamic Road Data

The digital information environment

The operational environment of SAE Level 4 automated freight vehicles is governed not only by the physical infrastructure they traverse, but also by the regulatory and dynamic informational environment that:

- defines permissible behaviour,
- communicates active conditions and
- signals changing circumstances along the route.

For a human driver, this environment is interpreted through:

- visual perception of physical signs,
- road markings and variable message displays, supplemented by tacit knowledge and
- contextual judgement.

For automated vehicles, the equivalent input should be available in digital, machine-interpretable form – delivered reliably, at the required quality level and through standardised interfaces [46] [47] [52] [54] [59].

The recommendations in this card address three complementary layers of this information environment:

1. the static provision of traffic rules and regulations in machine-interpretable formats,
2. the real-time provision of dynamic road, traffic and event data, and
3. the standardisation of infrastructure-to-vehicle communication services and the underlying Application Programming Interface (API) structures through which they are delivered.

Machine-interpretable traffic rules and regulations

The provision of traffic rules and regulations in machine-interpretable formats is a foundational facilitator for automated vehicles that must navigate legally across multiple national jurisdictions.

Road authorities and relevant jurisdictional entities are the authoritative actors for establishing traffic rules and traffic regulation orders. For automated vehicles, these rules cannot remain available only through human-readable signs or implicit legal knowledge; they should be represented as trustworthy, timely, authoritative and machine-interpretable information and made accessible through secured dissemination interfaces [46] [52] [54] [59].

This requirement follows from:

- the functional need of automated vehicles to understand applicable rules before and during operation, and
- from project evidence showing that vehicle-based sign detection and existing sign databases are not sufficiently reliable as the sole basis for regulatory compliance [59].

Ongoing European initiatives, including NAPCORE [11], the ITS Directive [12] and the emerging METR standardisation framework [13], provide a developing basis for aligning the digital and physical representation of traffic rules, but the level of completeness, cross-country consistency and machine readability required for SAE Level 4 deployment has not yet been achieved at corridor scale [52] [59].

Dynamic road, traffic and event data

The second layer concerns dynamic road, traffic and event data such as:

- roadworks,
- lane closures,
- temporary speed restrictions,
- hazardous situations,
- traffic signals,
- congestion and
- temporary changes to the physical layout of the road or logistics environment.

This category presents challenges because the events themselves are inherently time-bound, geographically variable and often not reflected promptly in static map data or sign databases. Project findings confirm that CCAM vehicles should have access to both static and dynamic information during public-road driving, and that dynamic information such as variable speed limits, temporary

roadworks and closed lanes should be provided by road authorities/road operators in machine-interpretable form so that vehicles can understand changes in driving conditions [46] [47] [52] [54] [56]. The same findings also distinguish between:

1. dynamic information distributed by road authorities and
2. information retrieved from roadside units in areas such as intersections, on- and off-ramps and blind spots created by changes in slope or curvature.

Safety-critical information, such as hazard warnings, must be prioritised over non-safety-critical messages and addressed immediately; automated vehicles therefore need to recognise the urgency of received dynamic information and prioritise it accordingly.

Standardised interfaces and information services

The third layer addresses the standardisation of the interfaces through which this information reaches the vehicle.

Infrastructure-to-vehicle real-time information services have been defined and standardised to a considerable degree within existing European C-ITS frameworks. European platforms like C-Roads [9] and C2C CC [10] provide harmonized C-ITS specifications and services. The challenge is not, therefore, primarily one of inventing new message types, but of ensuring that [52] [54] [59]:

- these services are consistently deployed,
- the underlying data sources such as VMS feeds, traffic management centre outputs and road authority data systems are regulated as infrastructure services with defined quality, availability and service-level requirements, and
- the API structures through which they are delivered are standardised to allow interoperable access across jurisdictions, vehicle platforms and operators.

RC-DI-3	Data Quality, Relevance and Feedback												
Stakeholder	AVO	AVU	**CB**	**DIA**	**DSP**	**PIA**	PIO	RO	SSP	TSP	TSU	**VM**	SIR

Main Challenges Addressed:

- Undefined data-quality, confidence, latency and availability requirements for digital infrastructure services
- Information overload and unstable behaviour from unfiltered V2X/cloud data
- No structured feedback loops for discrepancy reporting and data correction

Recommendations

- DI-09 — Define data-quality, confidence, stability, latency and availability requirements for digital infrastructure services used by automated freight vehicles.
- DI-10 — Apply intelligent filtering and relevance management to V2X, infrastructure and cloud data to avoid information overload and unstable system behaviour.
- DI-18 — Establish digital feedback loops between traffic management centres, road authorities, infrastructure operators and automated vehicle operators, including discrepancy reporting, data correction and quality feedback where relevant.

Estimated deployment / time horizon

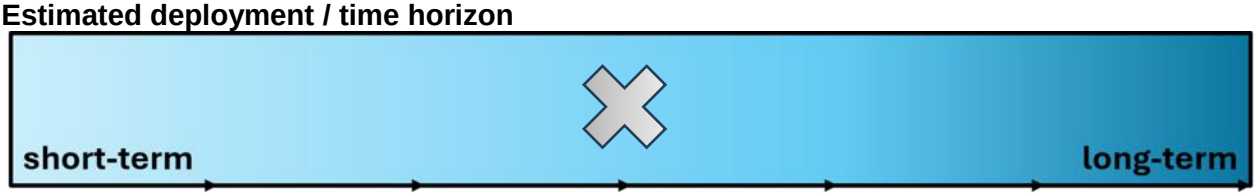


Figure 12: Recommendation Card: Data Quality, Relevance and Feedback

Data quality requirements for digital infrastructure services

The preceding recommendation cards in this chapter describe the content and technical configuration of digital infrastructure services for automated freight:

- connectivity architecture,
- geospatial data layers,
- machine-interpretable traffic rules and real-time event feeds.

These services are only operationally useful, however, if the data they deliver [47] [54] [59]:

- meets defined quality thresholds,
- is filtered to what is relevant for the vehicle's decision-making context, and
- is subject to systematic correction when errors or discrepancies are identified.

The rationale for defining explicit data-quality requirements (DI-09) follows directly from the functional role that infrastructure data plays in automated vehicle systems.

Infrastructure data serves as a valuable additional input to vehicle decision-making – extending situational awareness beyond onboard sensor range, providing regulatory context and supporting redundancy – but safety-critical decisions remain the responsibility of the vehicle system itself. This allocation of responsibility, which reflects both legal requirements and sound system design principles, implies that the vehicle needs to be able to assess the quality and confidence of incoming infrastructure data and to act appropriately when quality falls below an operational threshold [47] [54] [56]. Without defined quality, availability and latency requirements for each category of digital infrastructure service, the vehicle system cannot make such assessments in a principled way.

Data filtering and relevance management

Data filtering and relevance management (DI-10) addresses a distinct but complementary challenge that arises at scale. V2X communication, and the C-ITS services carried over it, are designed to support improved decision-making by connecting vehicles with:

- other vehicles,
- infrastructure,
- road users,
- traffic management systems, and
- network-based services.

The project's connectivity work confirms that V2X messages differ in type and format depending on the information carried and the service supported, and that application-level standardisation is required so that vehicles, infrastructure and other entities can interpret and use the information consistently across communication technologies [47] [54] [56]. This has direct implications for relevance management: filtering cannot be implemented as an ad hoc vehicle-specific function only, but must operate on standardised message semantics, service definitions and quality indicators that remain interpretable across ITS-G5, C-V2X, cellular and cloud-based delivery paths. The coexistence of different communication technologies further reinforces this requirement.

As automated vehicles receive and process data from multiple simultaneous sources intelligent filtering and relevance management is a safety and stability requirement since the vehicle system must be able to determine:

- which incoming data is relevant,
- what confidence level to assign to it, and
- when to discard or deprioritise data that does not meet operational thresholds.

This is particularly important in dense V2X environments and at transitions between infrastructure domains where the vehicle is simultaneously receiving data from multiple national, operator-specific or technology-specific sources. [47] [54] [56] [59]

Structured feedback loops

The third recommendation, DI-18, addresses the systemic quality assurance that lies outside the vehicle itself. Even well-specified services with defined quality requirements will produce errors, discrepancies and degradations over time.

For instance:

- road sign databases will become outdated,
- roadworks notifications will be published with incorrect geometry,
- correction service coverage will lapse.
- permanent traffic regulations will change without the relevant map or database being updated.

Automated freight vehicles, by virtue of operating continuously and systematically along defined corridors, are structurally well placed to detect such discrepancies – between what the digital infrastructure reports and what onboard sensors observe – and to report them. Project findings confirm that the value of such reporting is broadly recognised: road operators identify improved real-

time insight into the actual state of road infrastructure as a primary benefit of increased data exchange with vehicle operators, particularly for roadworks management and maintenance prioritisation [52] [54]. The operational reliability of real-time and near-real-time traffic management services was identified as the primary challenge for real-time collaborative traffic management schemes, with the availability and accuracy of data from road infrastructure sensors and traffic management systems as the main limiting factor. Structured digital feedback loops provide a mechanism for closing this gap on an ongoing basis.

5.2.2 Positioning and Mapping

Depending on the system design, accurate, consistent and machine-interpretable geospatial data is a structural need for lane-level path planning, localisation and regulatory compliance in SAE Level 4 automated freight transport. This section addresses the digital geospatial foundation on which multiple other infrastructure services depend:

- a common lane-level road network,
- standardised HD maps covering both public roads and confined logistics areas, and
- harmonised geodetic reference frames that ensure consistency across map, positioning and C-ITS data sources.

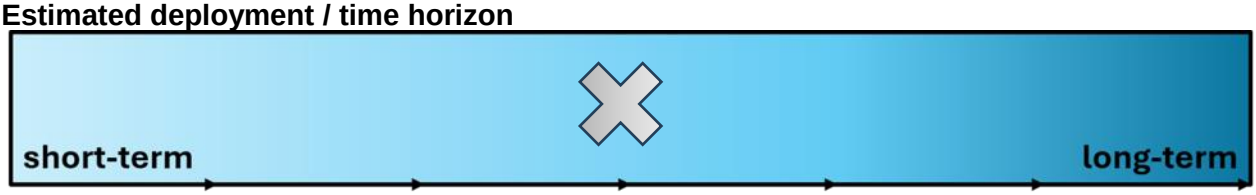
RC-DI-4	**Digital Maps, Positioning and Road Network**												
Stakeholder	AVO	AVT	**CB**	**DIA**	**DSP**	**PIA**	PIO	RO	SSP	TSP	TSU	**VM**	SIR
Main Challenges Addressed: • Lack of a trusted, lane-level base layer for routing and operational planning • Inconsistent HD map formats, quality and update processes, especially for confined areas and temporary situations • Fragmented geodetic reference frames, datums and metadata across map, positioning and C-ITS sources													
Recommendations • DI-03 — Establish a common lane-level digital road network as a trusted base layer for automated freight routing and operational planning. • DI-04 — Standardise HD map formats, quality requirements, governance models and frequent update and quality-assurance processes, including for confined areas such as ports and terminals as well as for temporary traffic management and construction sites. • DI-15 — Harmonise geodetic reference frames, map datums, elevation models, metadata and timestamps across map, positioning and C-ITS data sources.													
Estimated deployment / time horizon 													

Figure 13: Recommendation Card: Digital Maps, Positioning and Road Network

Geospatial data for automated freight

Automated freight vehicles operating at SAE Level 4 require a geospatial data environment of substantially greater precision, completeness and consistency than that needed for conventional navigation or driver-assistance applications.

The recommendations in this card address the digital geospatial foundation on which other digital infrastructure services depend:

- a trusted lane-level road network as a common base layer,
- standardised and regularly updated HD maps covering both public roads and confined logistics areas, and
- harmonised geodetic reference frames that ensure consistency across map, positioning and C-ITS data sources.

Common lane-level digital road network and governance

The need for a common lane-level digital road network stems from the functional requirements of automated routing and operational planning. Automated freight vehicles must be able to compute precise and unambiguous routes at the level of individual lanes, including lane geometry, topology, access restrictions, signage, traffic rules and the relationship between drivable and non-drivable space [52] [53] [59]. This level of detail is required not only on motorways and public road approaches, but also in confined logistics environments, where vehicles must execute precise manoeuvring sequences for gates, yards, loading positions, docking areas, coupling or uncoupling operations and transitions between public and private infrastructure domains. A common base layer should therefore be sufficiently standardised to support interoperability across vehicle systems, map providers, logistics operators and infrastructure authorities, while remaining extensible enough to incorporate local operational constraints and dynamic changes.

The governance of this base layer is as important as its technical specification. Project findings indicate that no single actor can provide and maintain the required geospatial environment in isolation:

- public road authorities and road operators are naturally positioned to maintain authoritative static datasets for public roads, while terminal operators and logistics-site owners are essential sources for confined-area layouts, access rules and operational constraints.
- Map providers and technology suppliers can transform these inputs into vehicle-usable map products and overlays, while vehicle operators and automated-driving system providers require reliable access to the resulting data and interfaces.

The resulting governance model should clarify responsibilities for provision, maintenance, update approval, liability, auditability and access conditions. Base data should be made accessible under secure and interoperable conditions, while sensitive confined-area or operationally specific data may require role-based access, contractual arrangements, authentication and traceable change management. [53] [54]

HD maps and lifecycle management

HD maps represent the precision layer that enables localisation, trajectory planning and operational decision-making within this common network.

They should provide:

- lane-level accuracy,
- robust semantic content,
- quality metadata and
- interfaces suitable for automated-driving systems, remote operation, fleet management and logistics planning.

MODI has demonstrated the value of multi-layer map structures combining localisation layers such as point clouds, road-geometry layers for path planning, and environment layers distinguishing drivable from non-drivable areas. However, scalable deployment requires moving beyond project-specific implementations towards standardised formats and interfaces, such as OpenDRIVE [14], Lanelet2 [15], NDS [16], DATEX II [16], C-ITS-compatible data structures and point-cloud formats where appropriate [52] [53][54] [59]. These standards must define not only data structure, but also:

- quality thresholds for accuracy,
- completeness,
- latency,
- reliability,
- temporal validity and consistency with vehicle sensor inputs such as GNSS, RTK/NRTK corrections, LiDAR, radar and camera perception.

Map quality cannot be treated as a one-time production task. HD maps are operational assets that must be validated, updated and quality-assured throughout their lifecycle.

Static road geometry may be updated periodically, but safety-relevant changes such as roadworks, lane closures, temporary barriers, altered terminal layouts, access restrictions, construction sites or changed traffic-management measures require rapid, event-driven updates. Update processes should therefore support automated and bidirectional data exchange, allowing infrastructure operators and site owners to publish authoritative changes while vehicles and fleets provide discrepancy reports or sensor-based feedback [52] [53] [54]. Critical updates should be distributed through standardised APIs and secure push/pull mechanisms, supported by:

- metadata,
- timestamps,
- audit trails and
- plausibility checks.

In confined areas, where layouts may change more frequently than on public roads, these update and governance processes are particularly important for avoiding operational discontinuities between the map, the physical environment and the vehicle's ODD.

Geodetic consistency across systems and borders

The third dimension of the geospatial foundation concerns geodetic consistency. Map data, GNSS correction services and C-ITS data sources each rely on reference frames, coordinate systems, elevation models, timestamps and metadata conventions. If these assumptions are not harmonised, otherwise accurate datasets can become misaligned when used together, particularly at borders, infrastructure-domain transitions or handover points between correction-service providers. Along a cross-border corridor, even small differences in national realisations of European reference frames can be relevant for lane-level localisation and automated manoeuvring. Harmonising geodetic reference frames, map datums, elevation models, metadata and timestamps is therefore necessary to ensure that HD maps, positioning corrections and cooperative infrastructure messages describe the same physical environment in a mutually consistent way. [52][58] [59]

5.2.3 Remote Operations

The operational management of SAE Level 4 automated freight extends beyond the vehicle to encompass the digital systems through which it is planned, supervised, recovered and admitted to access-controlled facilities. This section addresses the standardisation and governance requirements for this operating layer: the interfaces between automated vehicles and logistics systems, the coherent digital environment that integrates mission management with remote supervision and exception handling, and the trusted-process infrastructure that enables secure, uninterrupted passage through gates, terminals and customs checkpoints without the physical driver who has historically mediated these interactions.

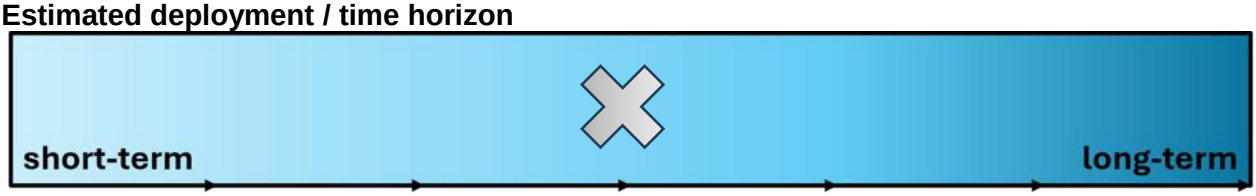
RC-DI-5	**Logistics and Fleet Digital Integration**												
Stakeholder	AVO	***AVU***	CB	DIA	***DSP***	FIA	PIO	***RO***	SSP	***TSP***	***TSU***	***VM***	SIR
Main Challenges Addressed: • Non-standardised interfaces between vehicles and logistics systems (TMS, FMS, WMS, TOS, RVOS, yard systems) • Fragmented mission, fleet, ETA, supervision and exception-handling functions • Missing machine-interpretable charging availability, booking and capability information													
Recommendations • DI-07 — Standardise interfaces between automated vehicles and logistics systems, including TMS, FMS, WMS, TOS, RVOS, yard systems and control towers. • DI-08 — Integrate mission management, fleet orchestration, ETA management, remote supervision, exception handling and recovery into a coherent digital operating environment. • DI-13 — Provide machine-interpretable information on charging availability, access, booking, pricing, connector compatibility and automated charging capabilities.													
Estimated deployment / time horizon 													

Figure 14: Recommendation Card: Logistics and Fleet Digital Integration

Logistics system integration and interface standardisation

The operational value of an automated freight vehicle is realised only to the extent that it is integrated into the wider logistics system in which it operates. A vehicle capable of SAE Level 4 automated driving on a defined corridor remains dependent, at every stage of its journey, on digital interfaces through which it:

- receives mission instructions, route assignments and operational documentation from carrier, fleet or terminal systems;
- reports status and progress back to logistics operators;
- it is supervised and remotely operated where necessary.

Without standardised, interoperable interfaces connecting the automated vehicle to the full range of systems it interacts with, each deployment requires bespoke integration work that neither scales across operators nor supports cross-border interoperability.

At the same time, logistics operators already rely on established:

- Transport Management System (TMS),
- Fleet Management System (FMS),
- Warehouse Management System (WMS),
- Terminal Operating System (TOS),
- yard systems and
- control towers,

many of which are legacy systems with long replacement cycles and site-specific configurations.

Standardisation should therefore not assume that these systems will be replaced or fundamentally redesigned for automated freight. Instead, it should focus on common data models, APIs and integration layers that allow automated vehicles and their supporting services to exchange the required information with both existing and future logistics systems. Where existing systems cannot directly support standardised interfaces, adapters, middleware or gateways may be required to translate between proprietary formats and the common interface. [53] [54]

Standardised interfaces and the role of the Remote Vehicle Operation System (RVOS)

The interface between the automated vehicle and the logistics operating environment is one of the most operationally consequential and least standardised digital connections in the automated freight chain.

According to DI-07 this standardisation should be improved. In a manually operated vehicle, the driver often functions as the integration point:

- receiving instructions,
- reporting progress,
- handling deviations and
- coordinating locally with terminal or fleet personnel.

In an automated vehicle, these functions must be mediated through digital interfaces between the vehicle, fleet systems, yard and terminal systems and remote operation systems. The validated interface architecture clarifies this relationship by positioning the RVOS as the system responsible for managing the mission of a single vehicle and for interacting with existing fleet management and

yard operation systems to gather the strategic information needed for a complete business trip [46] [54].

The RVOS translates strategic information from these systems into instructions that the automated-driving-equipped vehicle can handle, for example by:

- converting a yard destination into a GNSS position and heading,
- performing route planning,
- and managing vehicle-related business processes such as loading, unloading and charging.

This makes the RVOS a key integration layer between existing logistics systems and the vehicle, while also confirming that existing fleet and yard systems must be digitally adapted if they are to support automated operation at scale. [46] [54]

Coherent digital operating environment

The coherent digital operating environment addressed by DI-08 extends this integration to the operational management functions that must work together in real time: mission management, fleet orchestration, ETA management, remote supervision, and exception handling and recovery. MODI findings specify that an automated freight vehicle must be able to receive and act on a mission plan containing destinations, route, desired behaviour and actions to be executed at specific waypoints and must be able to receive updated plans when circumstances change. [46] [54]

Monitoring is distributed across system roles, with the vehicle responsible for its own operational status and ODD conditions and the RVOS responsible for mission health and progress. Remote supervision and remote operation are embedded as operational functions within this architecture, with the RVOS able to issue remote support or remote driving assignments and maintaining supervisory authority over the vehicle even when yard or terminal systems provide high-level mission instructions [46] [54]. This avoids ambiguous authority chains between fleet, terminal and remote-operation actors, and reinforces the need for traceable, role-specific interfaces for supervision, mission updates and recovery.

Machine-interpretable charging information

The third recommendation addresses a structurally essential dimension of fleet integration, that is the machine-interpretable provision of:

- charging availability,
- access,
- booking,
- pricing,
- connector compatibility and
- automated charging capabilities.

For heavy-duty electric vehicles on multi-country corridors, charging is a mission-critical logistical constraint. The remote operator requires continuous visibility of vehicle charging status, route and position, and must be supported when a planned charger is unavailable or charging fails [46] [48].

Without interoperable, machine-interpretable charging data accessible to TMS and mission planning platforms, logistics operators cannot reliably integrate energy constraints into route and schedule planning, and the resulting cost and availability uncertainty undermines the business case for large-

scale deployment. Together, the three recommendations define the digital operating environment without which automated freight cannot be operationally integrated into existing logistics chains, regardless of the vehicle's technical capability.

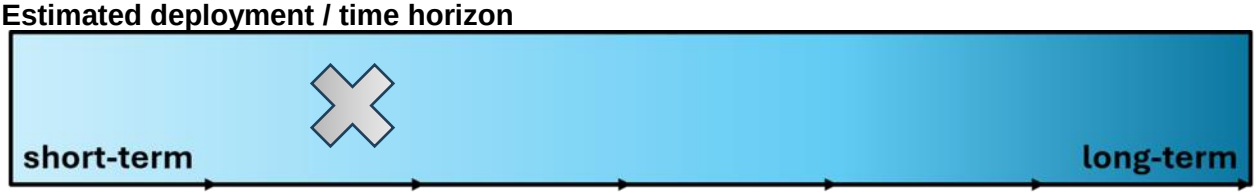
RC-DI-6	Digital Security and Trusted Processes												
Stakeholder	AVO	AVT	**CB**	**DIA**	**DSP**	**PIA**	PIO	RO	**SSP**	**TSP**	TSU	VIT	SIR
Main Challenges Addressed: • Manual identity and access checks that are unsuitable for unmanned operation • Safety-critical operations exposed to tampering and unauthorised access • Paper-based or pre-arrival-incompatible gate, customs and access-control processes													
Recommendations • DI-11 — Implement secure digital identity and cyber-secure authentication for vehicles, trailers, cargo, transport orders and access permissions, to avoid manual checks and to protect safety-critical operations against tampering and unauthorised access. • DI-12 — Digitise gate, customs, access-control and pre-clearance processes before vehicle arrival, including support for digital documentation such as eCMR.													
Estimated deployment / time horizon 													

Figure 15: Recommendation Card: Digital Security and Trusted Processes

Digital identity

The transition to SAE Level 4 automated freight fundamentally changes the trust and identity infrastructure required at access-controlled environments. In a manually operated vehicle, access control at terminal gates, port facilities and customs checkpoints often relies on physical interaction: a driver presents documents, enters a code, uses a tag or card, is recognised by a camera system, or communicates with a guard or local access control personnel [53][57]. These methods are structurally difficult to reconcile with unmanned operation, which has no driver available to perform manual tasks or resolve exceptions locally. At the same time, the absence of a physical driver increases the importance of secure digital interfaces between the vehicle, access-control infrastructure, backend management systems, remote-operation functions and logistics systems [46] [47] [53]. The two recommendations in this card address both dimensions:

- DI-11 establishes the secure digital identity and authentication layer that enables automated vehicles to operate in access-controlled environments without manual checks, and
- DI-12 applies this layer to the digitisation of gate, customs, access-control and pre-clearance processes so that access and compliance decisions can be prepared before the vehicle arrives and executed without driver intervention.

Digital identification and authentication

DI-11 responds to the operational gap between existing access-control infrastructure and the requirements of unmanned vehicles.

Project evidence confirms that logistics hubs, ports and warehouses use gates to regulate the entry and exit of vehicles, goods and personnel, and that traditional manual systems usually depend on personnel inspecting and releasing vehicles at the gate [57]. In a CCAM system, these functions need to be digitalised through connectivity technologies. To pass through a gate, the automated vehicle must be able to provide the necessary information to identify itself and justify the purpose of its visit, while the gate and its backend management system must assess the request and inform the vehicle whether access has been granted or rejected.

The project material identifies several possible technical approaches for this access-control function, each with different implications for security, robustness and interoperability [46] [47] [53]:

- Dedicated short-range communication systems can use a tag mounted in the vehicle and a reader installed behind the gate; this approach is described as cryptographically secure and associated with a very low misidentification rate, provided that the installations allow reliable detection when the vehicle stands in front of the gate.
- Camera-based licence plate recognition can also support access control, but its reliability depends on unobscured visual conditions and can be significantly reduced by adverse weather such as snow or heavy rain.
- C-ITS-based access can allow the vehicle's on-board unit to communicate with roadside equipment in the confined area using ITS-G5 or C-V2X, with the vehicle using positioning information to determine its proximity to the gate and sending location and identification information to the roadside unit.

After access approval, the roadside unit may open the gate directly or request a central system or manual operator to do so. Telematics-based access through a fleet-management back office is another possible pathway, using mobile-network connectivity between the vehicle and the gate via existing telematics infrastructure. These alternatives show that the core requirement is not tied to a single technology, but to a trusted, interoperable and secure mechanism for vehicle identification, access-request handling and backend authorisation.

Where gate access is not fully automated, an automated vehicle may need to stop and alert a remote intervention operator, who can interact with on-site access-control systems or personnel. This fallback option confirms the operational need for remote intervention but also illustrates why fully digitalised and trusted access processes are preferable for scalable automated freight: each unresolved manual dependency becomes a potential stop, delay or exception case. [48] [53]

Further, Cybersecurity is a prerequisite for the reliability and trustworthiness of these digital processes. Identity, authentication and access-control systems should therefore protect vehicles, infrastructure and backend services against unauthorised access, identity spoofing, manipulation of access requests, data interception and disruption of service. This requires secure communication, robust authentication and authorisation, protection of credentials and cryptographic keys, continuous monitoring, incident response and secure software and certificate management throughout the system lifecycle [46] [47] [54].

Digitised processes and pre-clearance

DI-12 addresses the process layer that surrounds identity and authentication. Gate access is not only a technical act of opening a barrier; it is part of a broader logistics and compliance process involving:

- planning,
- timing,
- routing to the correct gate,
- queuing or waiting,
- entry and exit from the gate area,
- vehicle and company identification,
- transport booking and,
- where relevant, customs documentation.

MODI findings show that gate-access processes may require information on the company or transport service provider, driver or vehicle identity, booking purpose at the terminal, timeslot booking, trailer pick-up or drop-off instructions, and documentation handling before arrival [46] [53] [54]. In an unmanned vehicle context, the question becomes whether information that is currently handled by a driver can be registered in advance, digitally associated with the vehicle and transport order, and made available to access-control and terminal systems before the vehicle reaches the gate. This is the operational basis for pre-clearance: access and routing decisions should be made from verified digital information before arrival rather than through ad hoc interaction at the gate.

5.3 SAE Level 4 integration in logistics

The deployment of SAE Level 4 automated freight vehicles in operational logistics settings requires not only a technically capable automated driving system, but also a coherent set of operational, organisational, and socio-technical conditions. While the preceding chapters on physical and digital infrastructure address the environment in which the vehicle operates, this chapter concerns the conditions under which the vehicle and the surrounding logistics system can function as an integrated operational whole. The seven recommendation cards cover deployment strategy and the definition of Operational Design Domains, operational readiness and safety assurance, remote operation and human factors, end-to-end logistics integration, validation methodology and requirements management, business models and organisational change, and the foundations for public trust and societal acceptance.

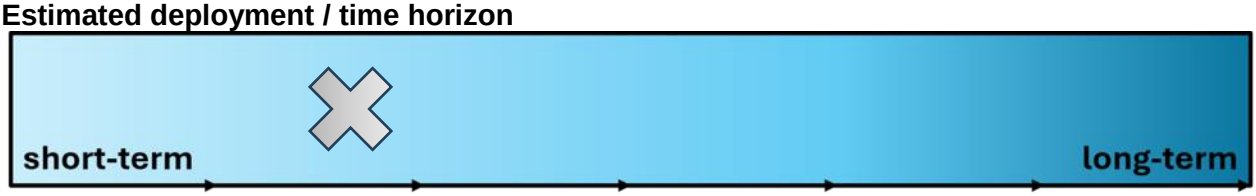
RC-L4-1	**Deployment Strategy and ODD Definition**												
Stakeholder	***AVO***	***AVU***	***CB***	*DIA*	*DSP*	*PIA*	*PIO*	*RO*	*SSP*	***TSP***	*TSU*	***VM***	*SIR*
Main Challenges Addressed: • Choosing suitable early use cases and routes for SAE Level 4 freight • Managing the steps from simple, controlled scenarios to complex, mixed-traffic environments													
Recommendations • L4-01 — Prioritise early SAE Level 4 freight deployment on high-volume, predictable point-to-point routes (A to B) with a simple, well-defined ODD. • L4-02 — Define ODD and TOD boundaries in a performance-based and graduated way rather than as binary operate/no-operate conditions. • L4-07 — Start with simple, controlled and repeatable operational scenarios and scale gradually towards more complex environments and mixed-traffic interactions													
Estimated deployment / time horizon 													

Figure 16: Recommendation Card: Deployment Strategy and ODD Definition

Prioritising early deployment use cases

The decision of where and how to begin large-scale deployment of SAE Level 4 automated freight represents one of the most consequential early choices in the commercialisation of automated logistics. Project evidence consistently demonstrates that the strongest and most credible early business cases arise from:

- repetitive, high-volume operations in confined areas (e.g. mining, port terminals, industrial areas) or
- in point-to-point logistics flows – shuttle routes between warehouses, port-hinterland corridors and hub-to-hub operations with well-defined, stable operational environments [45].

The commercial logic is straightforward: on high-volume, predictable routes where a vehicle operates the same sequence of road segments day after day, the marginal cost of automation

decreases with operational hours, while the variability of the environment (and with it the demand placed on the vehicle's automated driving system) remains bounded. Business-case evidence further indicates that such flows are attractive because they allow for high asset utilization in the face of constraints imposed by current SAE Level 4 CCAM technology, and with only limited orchestration of vehicle and logistics activities [45].

However, a simple or narrowly defined predictable route is not sufficient on its own to identify the most suitable early deployment cases. Use cases should also be assessed according to their potential to scale across the regulatory, safety, operational and business dimensions.

Priority should be given to deployment cases that combine:

- a manageable ODD with a credible approval pathway,
- demonstrable safety assurance,
- repeatability across routes or sites,
- limited dependence on bespoke infrastructure and integration, and
- a sustainable commercial model.

Such early-deployment-oriented use cases can generate operational value and evidence at comparatively low complexity, support investment decisions and establish reusable capabilities for the subsequent deployment of more complex applications.

A further criterion for early use-case selection is the extent to which the current driver role includes non-driving tasks. Use cases in which the driver is primarily responsible for the driving task, with few manual activities at the origin, destination or intermediate stops, may be deployable earlier because removing the driver requires comparatively limited adaptation of existing logistics processes. By contrast, use cases in which drivers also perform non-driving related tasks require the respective functions to be automated, digitalised, remotely supported or reassigned before fully driverless operation becomes feasible. The assessment of early deployment cases should therefore consider the complete operational role of the driver, rather than the driving task alone.

The MODI demonstrations showed that the value of SAE Level 4 freight transport lies in sustained public-road logistics operations in addition to controlled-area applications, and that the logistics context of the route shapes whether automation can deliver a robust and scalable operational case [59].

Graduated domain concepts

A necessary corollary to route prioritisation is the way ODD and Transfer of Control Domains are defined. Project findings indicate that current ODD definitions frequently operate as binary, operate-or-not-operate thresholds: a vehicle is either within its ODD and performing fully automated driving, or outside it and returning control to a human driver. Under this binary logic, even brief excursions beyond the ODD boundary e.g. due to weather, roadworks, temporary signage changes, etc., translate directly into unplanned operational downtime and reduced vehicle utilisation, with immediate consequences for economic viability [47] [55].

A performance-based and graduated ODD definition, i.e. one that specifies restricted operating modes, reduced speed envelopes, enhanced supervisory requirements, connectivity-dependent operating conditions or planned fallback procedures as intermediate states rather than forcing an immediate hand-back to manual operation, is therefore essential to maintaining vehicle utilisation

and operational continuity under the realistic variability encountered on long-distance freight corridors [47] [51] [59].

Such graduated ODD and Target Operational Domain (TOD) concepts also require architectural support at the interface between vehicle, infrastructure, communication services and supervision. MODI evidence indicates that ODD attributes should be:

- represented in a machine-interpretable form,
- monitored dynamically, and
- linked to boundary detection, operator notification and fallback logic [51].

The ability to continue automated operation therefore depends not only on the road geometry itself, but also on the availability and quality of digital and physical infrastructure layers such as HD maps, GNSS correction, RSUs, V2X/C-ITS services, mobile-network coverage and reliable cross-provider handover [47] [51]. Where these layers degrade, the system should be able to distinguish between conditions

1. that still allow automated operation with constraints,
2. that require remote supervision or tactical support, and
3. that require a minimal-risk manoeuvre or controlled stop [47] [51].

This reinforces the physical-infrastructure requirement that corridors and logistics sites cannot be assessed only as passable or impassable; they should be evaluated according to the operational modes they can support, the fallback locations available, and the continuity of the physical–digital interface along the route [51] [59].

Sequencing operational complexity

The third element of this card addresses the sequencing of operational complexity. Project demonstrations across all five use cases operated along a consistent pattern: successful demonstrations began in environments that could be made sufficiently controlled, repeatable and well-characterised before expanding into scenarios with higher degrees of mixed traffic, environmental variability and cross-boundary interaction [56] [57].

- The Hamburg use case demonstrated that V2X-supported extensions to Level 2 systems represent a technically and regulatorily viable intermediate pathway that meaningfully expands the ODD while the full SAE Level 4 type-approval trajectory matures [56].
- The Swedish hub-to-hub demonstrations confirmed that confined-area environments such as logistics centres, port terminals and warehouse facilities, while insufficient as end-states for commercial scale, provide a controllable context in which vehicles, remote operators and logistics workflows can be systematically validated before exposure to the full complexity of public-road mixed-traffic scenarios [57].

These environments are particularly important for validating physical interfaces such as gates, loading areas, docking positions, charging spaces, access-control points and terminal layouts, where automated vehicles must interact reliably with logistics processes rather than merely drive within a bounded area [57].

RC-L4-2	Operational Readiness and Safety Assurance											
Stakeholder	***AVO***	***AVU***	***CB***	***DIA***	***DSP***	***PIA***	***PIO***	***RO***	***SSP***	***TSP***	***TSU***	***VM***	***SIR***

Main Challenges Addressed:

- Lack of standardised operational-readiness frameworks (safety cases, go/no-go, incident response)
- Exception handling, recovery and restart treated as secondary rather than core capabilities

Recommendations

- L4-03 — Use standardised operational-readiness frameworks covering safety cases, go/no-go criteria, risk assessment, incident response and operational approval.
- L4-04 — Govern exception handling, recovery, fallback operation and restart procedures as core deployment capabilities and demonstrate validated degraded-mode, connectivity-loss and emergency-fallback behaviour, since how the system behaves in these situations strongly influences public trust and acceptance.

Estimated deployment / time horizon

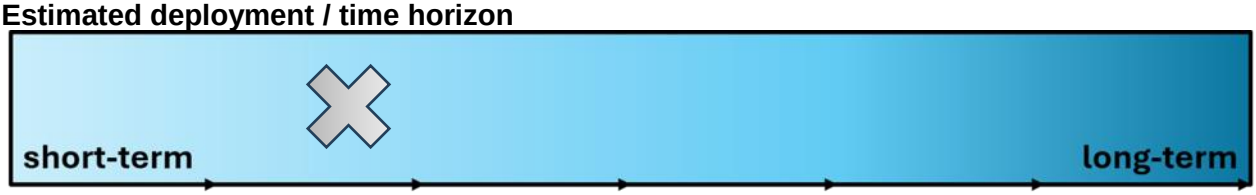


Figure 17: Recommendation Card: Operational Readiness and Safety Assurance

Operational readiness frameworks for automated freight deployment

The transition from technical feasibility to operational deployment of SAE Level 4 automated freight systems is not only a technology problem. MODI demonstrated that an additional gating factor is operational readiness: the capacity to document, demonstrate and formally certify that a system can operate safely under the full range of conditions it will encounter in service [58].

Across the MODI use cases, the preparation required before a single demonstration could take place on public roads amounted in the most complex case to nearly three years of work [58].

This experience confirms that standardised operational-readiness frameworks could heavily facilitate the deployment process: without them, each deployment must negotiate its own safety gate from first principles, duplicating effort, introducing inconsistency across jurisdictions, and lengthening the timeline between technical readiness and commercial operation.

HMI and communication-system readiness

Operational readiness also depends on whether the vehicle, in-vehicle interface and remote-operation interface can make the system's operational state visible and actionable to the responsible human actor.

Project evidence indicates that the interface must communicate system status, degraded modes, warnings, readiness conditions and mode transitions in a way that enables operators to:

- monitor the vehicle,
- understand whether deployment preconditions are still fulfilled, and
- intervene when required [48].

This includes the communication of real-time telemetry, maintenance or delay warnings, loading or docking readiness, and conditions that determine whether an operation may proceed or must be halted [48].

These interface requirements form part of the safety evidence for operational approval, because a go/no-go framework cannot be implemented reliably if the operator cannot determine whether the vehicle is ready, degraded, outside its authorised operating conditions, or in need of fallback support [48] [58].

Communication-system readiness forms a parallel precondition for deployment. Project findings indicate that safe automated operation and safe transition between automated, manual and remote-supported modes require:

- reliable, low-latency and standardised connectivity, together with
- monitoring of quality-of-service parameters such as latency, throughput and message integrity [47].

Where connectivity, positioning or message integrity fall below the required threshold, the operational framework must treat this not as a minor service-quality issue but as a safety-relevant condition that can trigger degraded operation, fallback, recovery procedures or a controlled stop [47]. This means that deployment approval should not only assess vehicle performance in nominal conditions, but also whether communication loss, handover failure or degraded data quality are detected, communicated to the operator and handled through predefined procedures [47] [58]. In this sense, connectivity and HMI readiness are part of the same operational-readiness logic as safety plans and risk assessments: they determine whether the certified operating concept can be executed in service [47] [48] [58].

Exception handling, fallback and recovery

The second recommendation in this card addresses the dimension of operational readiness that is most consistently underestimated in deployment planning: the handling of exceptions, degraded modes, fallback operation and recovery.

Corridor assessments demonstrated that no information layer along the Rotterdam–Oslo route is uniformly reliable under all environmental and traffic conditions, meaning that any operationally deployed SAE Level 4 freight system will encounter situations outside its nominal ODD boundary during routine service [59].

Further, degraded-mode performance has the potential to shape public trust in automated freight systems more decisively than nominal-performance metrics, because the public forms its judgements primarily through observation of how systems behave when something goes wrong, not when everything works as expected (see Annex III: Trust, Human Factors and Public Acceptance in Level 4 Automated Freight Transport).

Exception handling, fallback operation and restart procedures should therefore be:

- treated as first-class deployment capabilities,
- subject to the same requirements management, testing and independent validation as the nominal automated-driving functions, and
- demonstrated to predefined performance thresholds under repeatable conditions before a safety case can be considered complete [59] [Annex III].

This includes the ability to

- notify operators of failures or mode transitions,
- trigger minimal-risk manoeuvres or safe stops where required,
- support manual or remote intervention where authorised, and
- document recovery or restart procedures after connectivity loss, technical failure or operational interruption [47] [48] [59].

Operational readiness is therefore not achieved when the automated vehicle can drive successfully through the intended route once; it is achieved when the deployment organisation can prove that the vehicle, operator, communication system, fallback concept and approval framework remain coherent when the operational environment deviates from plan [47] [48] [58] [59].

RC-L4-3	Remote Operation and Human Factors												
Stakeholder	***AVO***	***AVU***	*CB*	*DIA*	*DSP*	*PIA*	*PIO*	***RO***	*SSP*	*TSP*	*TSU*	***VM***	***SIR***

Main Challenges Addressed:

- Scalable remote-supervision and remote-operation concepts not yet defined (roles, workload, situational awareness)
- Operator-vehicle ratio is a key design parameter (influencing connectivity requirements, task distribution, personnel skills and total costs of ownership)
- HMI and human-factors requirements considered too late in system design
- Risk of remote-operator overload from poor alerting and task allocation
- External HMI and transparent communication with surrounding road users not yet explicit

Recommendations

- L4-05 — Develop scalable remote-supervision and remote-operation concepts, including operator roles, workload, situational awareness and intervention procedures, and define human-centred minimum requirements covering alarm prioritisation, staffing resilience, controllability, operator engagement monitoring and trust calibration to counter overreliance during stable operation.
- L4-12 — Include HMI and human-factors requirements for remote operators, on-site personnel and surrounding traffic participants from the beginning of system design, including external HMI for transparent communication with surrounding road users.
- L4-13 — Prevent remote-operator overload by designing clear alerts, prioritised information, ergonomic interfaces and appropriate task allocation.

Estimated deployment / time horizon

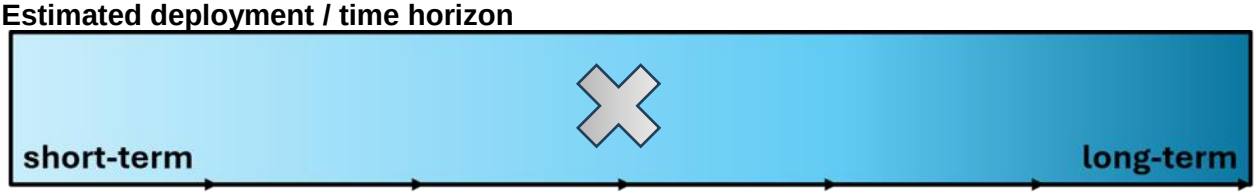


Figure 18: Recommendation Card: Remote Operation and Human Factors

Scalable remote operations and human oversight model

The commercial viability of SAE Level 4 automated freight transport depends not only on the automated driving capability of the vehicle but also on the scalability of the human oversight model that accompanies it.

Demonstrations conducted as part of the project showed that a remote operator is an active operational actor performing a wide and demanding range of tasks during every mission. The

transition from driver to remote operator is therefore rather a redistribution than a reduction of human involvement: the operator moves from physical vehicle control to mission-level decision support, situation interpretation and logistics continuity management [57] [58]. For this transition to be operationally scalable, the scope, structure and information environment of the remote operator's role must be deliberately engineered, not assumed to emerge from current practice.

MODI specifies this information environment in concrete terms. Remote operators require continuous situational awareness of:

- vehicle status,
- route and mission progress,
- surrounding conditions,
- alerts,
- cargo or logistics-process status, and
- live video or sensor feeds where these are necessary for supervision or intervention [48].

The remote interface should therefore support both: routine mission oversight and escalation. Therefore, it should:

- allow the operator to monitor automated task execution during stable operation,
- receive prioritised and actionable alerts at defined escalation points, and
- access intervention controls when an exception cannot be resolved by the automated system alone [48].

Functional architecture evidence further indicates that the remote operator is part of the mission-management system rather than an external add-on, requiring:

- secure and low-latency bidirectional communication between operator and vehicle,
- documented handover procedures between operators or operational domains, and
- scalable one-to-many supervision concepts where safety evidence supports them [51].

Preserving operational knowledge and designing effective interfaces

The effective design of scalable remote supervision concepts also requires that the knowledge base of experienced logistics and terminal personnel be systematically captured and made available to remote operators.

Project findings indicate that a significant portion of the efficiency and resilience of current terminal and drayage operations rests on tacit knowledge, i.e. informal, accumulated understanding of:

- site-specific routines,
- trailer positioning conventions,
- loading bay constraints, and
- the unspoken coordination signals through which drivers and terminal workers communicate

This tacit knowledge is difficult to formalise and harder still to transfer to a remote operator who may be geographically distant from the site and interacting with it only through camera feeds and digital system interfaces [58].

Recruiting remote operators with prior logistics or driver experience was identified as one approach to preserving operational situational awareness at the necessary depth [58]. More structurally, the design of remote supervision concepts should:

- incorporate explicit procedures for those elements of the logistics process that currently depend on human physical presence, informal judgment and on-the-spot flexibility
- define how these are to be performed from a remote position without loss of operational reliability [57] [58].

Human factors and HMI requirements should be defined at the outset of system design, not retrofitted once the automated driving architecture is already fixed.

MODI demonstrates that the operator's interface to the vehicle and its mission encompasses multiple functional layers:

- monitoring the vehicle's autonomous task execution,
- receiving requests for authorisation or intervention,
- overseeing the status of logistics sub-processes such as loading, unloading and access control, and
- communicating with on-site personnel and logistics systems [57].

These interfaces require:

- layered, context-sensitive information displays,
- prioritised and visually distinguishable alerts,
- ergonomic layouts and interaction designs that adapt to task complexity rather than presenting all available information with equal salience [48].

On-site personnel require similarly clear but simplified displays and interaction cues, because they need actionable information about vehicle intentions, readiness, access status or operational constraints without being burdened by the full remote-supervision interface [48].

Managing workload and cognitive overload

The third recommendation addresses the operational risk of remote-operator cognitive overload, which is a risk that is structurally embedded in the transition from one-to-one supervision to scalable fleet oversight.

Operators may develop a degree of overconfidence during stable motorway-phase operation, in which the automated system functions predictably and demands little active monitoring, only to be confronted abruptly with concurrent alerts when an unexpected situation, such as a road closure, a queuing event, a connectivity interruption, or a logistics process deviation (see Annex III). Interface requirements therefore emphasise:

- tiered alert severity,
- filtering of non-critical information,
- escalation logic,
- operator acknowledgement,
- notification logging and integration of alerts into the mission timeline, so that safety-critical events are distinguished from logistics-operational and informational notifications [48] [51].

Testing of remote-management HMI concepts further identified alert fatigue as a realistic risk and confirmed the need for response-performance benchmarks, adaptive alerting and workload balancing when operators supervise several vehicles or missions under realistic task conditions [50].

Taken together, these findings show that scalable remote supervision must be treated as a socio-technical operating capability. It requires:

- a defined operator role within the mission-management architecture,
- reliable and secure communication channels,
- clear handover and escalation procedures,
- HMI designs that support situational awareness without overloading the operator, and
- organisational models that preserve logistics knowledge while enabling one-to-many supervision if justified by evidence [48] [51] [57] [58].

RC-L4-4	End-to-End Logistics Integration and Vehicle Precision											
Stakeholder	***AVO***	***AVU***	***CB***	***DIA***	***DSP***	***PIA***	***PIO***	***RO***	***SSP***	***TSP***	***TSU***	***VM***	***SIR***

Main Challenges Addressed:

- Automation value lost where vehicles are not integrated into the end-to-end logistics system
- Insufficient vehicle precision for docking, charging, coupling and low-speed manoeuvring
- Technical development of vehicles and infrastructure elements not aligned with logistics workflows

Recommendations

- L4-06 — Design automated freight vehicles as part of an end-to-end logistics system – including loading, unloading, energy/charging, documentation, scheduling and yard processes – and develop the wider autonomous logistics ecosystem (including automated loading, unloading and charging suppliers) so that the end-to-end chain can operate without manual last-metre process breaks.
- L4-08 — Ensure high vehicle precision for docking, reversing, charging, coupling, loading and low-speed manoeuvring in logistics environments.
- L4-10 — Apply logistics-centred design methods and iterative V-model approaches to ensure that technical development involves alignment with logistics workflows.

Estimated deployment / time horizon

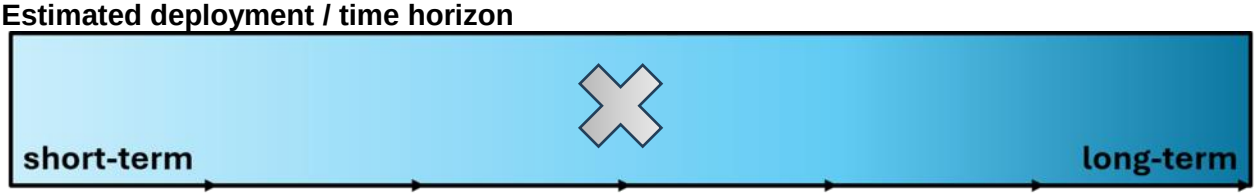


Figure 19: Recommendation Card: End-to-End Logistics Integration and Vehicle Precision

End-to-end integration into the logistics chain

The automated vehicle creates logistics value only to the degree that it is integrated into the broader operational chain of which it is one component.

A vehicle capable of automated driving on a defined route remains, at every boundary of its journey, dependent on the manual execution of surrounding processes unless those processes are also automated and digitally connected to the vehicle's operating environment.

MODI demonstrations indicated that across multiple sub-use cases, the automated vehicle itself performed its driving task reliably, while the value realised from its operation was disproportionately constrained by the manual or digitally disconnected state of upstream and downstream logistics processes [45] [57][54]. The perception that automating the vehicle is the primary task of automated freight deployment therefore underestimates the role of the wider logistics system in value creation [45].

End-to-end logistics integration therefore depends on a connectivity and interface layer that allows the automated vehicle to exchange operational data with logistics, yard, charging, documentation and remote-monitoring systems in real time [46] [47]. MODI identifies the need for standardised and secure interfaces between the vehicle and surrounding systems such as TMS, ERP, yard or terminal management platforms, loading systems, etc. [46] [47].

Such interfaces are needed to enable both:

1. **operational orchestration**, including vehicles, routes, terminal and warehouse activities, charging and remote supervision; and
2. **commercial orchestration**, including freight, goods, production and volume pooling

which will be critical for establishing business viability in a wide range of logistics operations [45].

As such these interfaces need to support more than passive status reporting: they should carry vehicle status, cargo and mission information, operational instructions, route or yard assignments, charging availability, documentation updates and exception information in a form that can be acted on by both the vehicle and the logistics system [46] [47].

Thus, the development of the autonomous logistics ecosystem is accordingly a prerequisite condition for end-to-end deployment at commercial scale, not a downstream consequence of vehicle deployment [45] [57].

Precision requirements in logistics environments

The precision requirements imposed on automated freight vehicles in logistics environments represent a distinct and demanding technical specification, separate from the highway-driving and urban-traffic capabilities that typically dominate vehicle development roadmaps.

The relevant low-speed logistics tasks include:

- reversing accurately into a loading dock;
- aligning the vehicle's cargo floor height with a ramp via air suspension adjustment;
- coupling to a trailer within the tight tolerances of automated coupling systems;
- navigating the constrained geometry of a yard or port terminal; and
- positioning precisely at a charging station for automated plug-in.

Each of these tasks requires high positioning accuracy and high-confidence environmental perception under conditions that systematically challenge sensor performance [57] [59].

MODIs Use Case demonstration indicates that such precision tasks require a combined vehicle–infrastructure approach. [46] [47]. Corridor assessments confirmed that lane detection performance degrades specifically during low-speed manoeuvres and when entering confined areas, precisely the operational contexts in which vehicle precision is most critical [59].

Further, demonstrations showed that remote operator intervention was currently required to complete several tasks such as adjusting suspension height, selecting and confirming dock alignment and verifying the safety of the docking approach, because the vehicle's autonomous positioning capability alone was not yet sufficient to execute them reliably without human oversight [57].

Infrastructure support at logistics nodes was identified as a necessary complement to on-board vehicle capability, since precision tasks at this level cannot be resolved by the vehicle in isolation from the physical and digital environment of the site [46] [47] [52] [57].

This requirement is especially important because the logistics site is not a neutral backdrop for automation and all particularities become part of the functional operating environment for the automated vehicle [57] [59]. Vehicle precision for logistics therefore requires both technical capability on board the vehicle and sufficient consistency, digital representation and machine-interpretable communication in the surrounding physical infrastructure [46][47] [57].

Logistics-centred and iterative system design

The third recommendation in this card addresses the process by which automated freight systems are developed, and specifically the risk that technical development proceeds on a vehicle-capability logic that is insufficiently connected to the operational workflows into which the vehicle will be inserted.

MODI showed that the largest sources of integration friction in automated freight deployments arise not from failures of the vehicle's automated driving system per se, but from mismatches between the vehicle's operating assumptions and the actual logistics environment:

- dock dimensions that differ from the vehicle's manoeuvrability envelope,
- yard routing protocols that assume manual driver judgment,
- scheduling workflows that assume a driver will resolve last-minute exceptions, and
- documentation processes designed around a physical person present at the vehicle [57] [58].

These mismatches are not discovered during laboratory development; they emerge during field integration, when the technical system first encounters the operational reality that was not fully represented in its requirements.

Project findings therefore support logistics-centred design methods that combine:

- workflow mapping,
- stakeholder co-creation,
- scenario-based impact assessment and
- iterative validation,

so that technical development is continuously checked against the business and operational processes it is expected to serve [55].

The logistics-centred design approach aligns CCAM design choices across four interdependent levels:

- vehicle and control systems;
- logistics processes and people;

- organisational structures and responsibilities; and
- laws and regulations.

Considering these levels together provides a no-regret approach to integrating CCAM into logistics, because it reduces the risk that improvements at one level create operational barriers or unintended consequences at another. Their alignment supports the identification of CCAM configurations that can maximise positive impacts on the efficiency, sustainability and safety of future transport operations.

An iterative V-model approach is particularly relevant because it links requirements definition, system design, verification and operational validation rather than treating logistics integration as a late-stage implementation task [55].

Under such an approach:

1. logistics workflows are translated into requirements;
2. these requirements are tested against technical system behaviour;
3. the resulting system is validated in realistic scenarios; and
4. identified misalignments are fed back into design decisions when they lead to manual intervention, delay, increased cost or reduced adoption potential [55].

The approach can also support the analysis of cost drivers through sensitivity analyses that account for uncertainties in technological development, system functionality and operational conditions. By exploring and comparing multiple CCAM designs – ranging from configurations close to current manned operations to more innovative or partial implementation concepts – logistics organisations can identify feasible transition pathways and determine where and how to take their first steps towards deployment.

The assessment should explicitly consider and weigh relevant impact indicators. Although total cost of ownership is often central to the business case, other factors may be equally important, including:

- personnel availability,
- operational efficiency,
- safety,
- sustainability,
- implementation complexity and
- resilience.

Comparing alternative CCAM designs against these indicators provides a more complete basis for selecting solutions that are technically feasible, operationally suitable and capable of being introduced progressively into existing logistics systems.

RC-L4-5	Validation, Testing and Requirements Management												
Stakeholder	***AVO***	***AVU***	***CB***	***DIA***	***DSP***	***PIA***	***PIO***	***RO***	***SSP***	***TSP***	***TSU***	***VM***	***SIR***

Main Challenges Addressed:

- Robustness, economics and acceptance not validated under real long-term conditions
- Use cases, functions, stakeholders and validation activities not traceably linked
- Complex operational environments and logistics edge cases not systematically covered in testing
- Structured closed-course/sandbox/simulation validation before public-road deployment, including human-system-interaction performance, not yet explicit

Recommendations

- L4-09 — Conduct long-term field trials under real operational, seasonal, traffic and weather conditions to validate robustness, economics and acceptance.
- L4-11 — Maintain structured requirements databases linking use cases, system functions, stakeholders, infrastructure needs and validation activities.
- L4-14 — Use scenario-based testing and edge-case documentation – including edge cases specific to logistics integration – and complete structured closed-course, sandbox and/or simulation validation programmes before public-road deployment, covering degraded modes, remote operations, connectivity loss and emergency fallback, independently validated against predefined thresholds and assessing both technical outcomes and human-system-interaction indicators (e.g. operator response quality and surrounding road-user interpretability).

Estimated deployment / time horizon

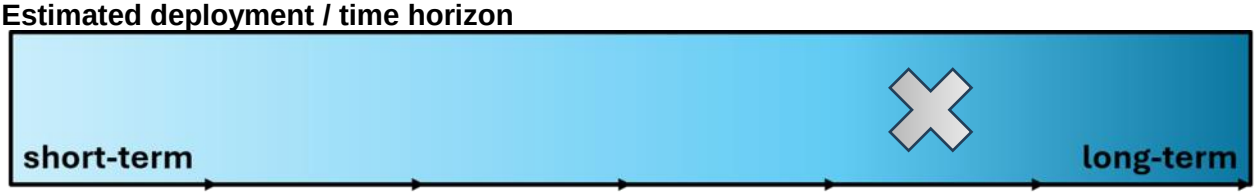


Figure 20: Recommendation Card: Validation, Testing and Requirements Management

Long-term field trials under real operational conditions

The validation of automated freight systems under real operational conditions is qualitatively different from performance measurement under controlled test settings. Project demonstrations consistently showed that controlled, bounded demonstration runs – conducted outside peak traffic hours, under permit-constrained weather conditions, on pre-cleared routes – reveal only a partial picture of the variability a deployed system will encounter in commercial service [56] [58].

Environmental limitations imposed by permit conditions in several use cases meant that:

- demonstrations could not proceed under rain, snow or high winds,
- traffic density was lower than the representative service conditions,
- routes were adjusted to reduce complexity relative to the original operational target [57] [58].

These constraints were operationally necessary to secure permits and manage safety risk during early-stage demonstrations, but they also mean that the resulting performance data cannot be directly extrapolated to the full range of conditions that a commercially deployed system would encounter across seasons, weather states and traffic environments [59].

Long-term field trials conducted under real operational conditions, including night driving, adverse weather, winter road states and normal traffic densities across all times of day, are therefore an

essential evidential foundation for robust operational claims [59]. These trials should assess not only the functionality and performance of the technology, but above all its integration into end-to-end logistics processes and the potential to optimise operations under representative commercial conditions. This includes evaluating interactions with logistics systems and personnel, process continuity, exception handling, resource utilisation, scheduling and the effects of automation on overall operational efficiency.

Project corridor assessments identified specifically that perception performance degrades under snowy conditions and during seasonal variation, and that operations should be conditioned to real quality variability with enable/disable logic tied to live quality indicators rather than fixed thresholds set during favourable test conditions [59].

Real-world testing additionally proved indispensable for discovering operational edge cases that theoretical simulations and controlled demonstrations failed to surface [57].

Structured requirements and traceable validation

The MODI findings demonstrated that the complexity of automated freight systems, which span vehicle hardware and software, digital and physical infrastructure, logistics operating systems, remote supervision functions, regulatory frameworks and safety cases, generates a requirements landscape that cannot be managed through informal documentation.

As the system evolves e.g. through over-the-air software updates or infrastructure changes traceability between requirements and their validated fulfilment must be maintained in a structured form that allows affected components and safety arguments to be identified and re-validated without rebuilding the entire case from scratch [Annex III].

Requirements databases, scenario libraries, unique identifiers, mapping tables and validation logs provide the practical mechanisms for maintaining this traceability across use cases, system functions, stakeholder dependencies, infrastructure assumptions and test outcomes [55][49].

A structured requirements database that explicitly links each use case to the system functions it activates, the stakeholders it involves, the infrastructure it presupposes and the validation activities that confirm its safe fulfilment provides the architectural backbone for a living safety case – a certification artefact that grows with the system rather than being frozen at a single point in time (Annex III). This is particularly important for cross-border and multi-site deployment, where comparable evidence is needed across differing physical infrastructure, digital services, regulatory conditions and operational roles [55][47].

Scenario-based validation and edge-case testing

The third recommendation in this card defines the validation methodology that must precede public-road deployment and has been significantly strengthened through project experience and human-factors analysis.

Scenario-based testing is the validation approach considered best suited to producing structured, repeatable and independently verifiable evidence that a system behaves correctly under conditions that may be rare in normal operation but consequential when they occur [59] [Annex III].

Scenario-based safety testing of adapted vehicles confirmed that validation must explicitly include ODD-boundary conditions, safety-critical edge cases and situations in which system behaviour depends on fallback logic or infrastructure support [50]. Testing at scenario boundaries revealed

operational gaps, fallback needs and system or infrastructure limitations that would not necessarily be visible in nominal demonstrations or in validation approaches focused only on controlled performance metrics [50]. These findings reinforce the need for scenario libraries that are continuously updated with edge cases discovered during field trials and linked back to the requirements database, so that validation evidence remains traceable as the system and operating environment evolve [50] [55] [59].

The extended formulation of this recommendation, informed by human-factors considerations, specifies that structured closed-course, sandbox and simulation validation programmes should also cover degraded modes, remote operation scenarios, connectivity loss and emergency fallback behaviour, and that they need to be independently validated against predefined performance thresholds covering both technical safety outcomes and human-system interaction indicators, including operator response quality and the interpretability of vehicle behaviour to surrounding road users (Annex III).

The recommendation also explicitly incorporates edge cases specific to logistics integration:

- complex trailer coupling approaches,
- automated loading failures,
- yard-routing deviations and cooperative merging in roadworks environments involving large vehicles with restricted line of sight.

Validation for automated freight therefore cannot be reduced to proving that the vehicle drives correctly in a preselected route segment; it must demonstrate that the integrated logistics, vehicle, infrastructure, communication and human-oversight system remains safe, interpretable and recoverable when operational conditions deviate from plan [47] [49] [50] [59].

RC-L4-6	Business Models, Value Networks and Organisational Change												
Stakeholder	***AVO***	***AVU***	***CB***	***DIA***	***DSP***	***PIA***	***PIO***	***RO***	***SSP***	***TSP***	***TSU***	***VM***	***SIR***

Main Challenges Addressed:

- Duplicated and inconsistent impact-assessment data requests from authorities
- Business-process change and tacit operational knowledge underestimated during automation
- Unclear value flows, responsibilities and risk distribution among enterprise objects
- Lack of long-term contractual and risk-sharing models to support investment

Recommendations

- L4-15 — Establish a unified, harmonised data-provision framework that aligns the impact-assessment data requested by authorities (ex-ante and ex-post), so that deployment decisions can be evaluated consistently against cost, safety, productivity, sustainability and service availability while reducing duplicated reporting effort for operators.
- L4-16 — Explicitly account for business-process change, tacit operational knowledge and workflow restructuring when introducing automated freight systems.
- L4-18 — Develop a value network for the enterprise objects involved in a MODI-like concept to clarify value flows, responsibilities, benefits, risk/vulnerability aspects and data needs for evaluation and quality control.
- L4-19 — Establish long-term contractual frameworks and risk-sharing models between shippers, logistics operators, OEMs, infrastructure providers and technology providers to support investment in scalable L4 freight systems.

Estimated deployment / time horizon

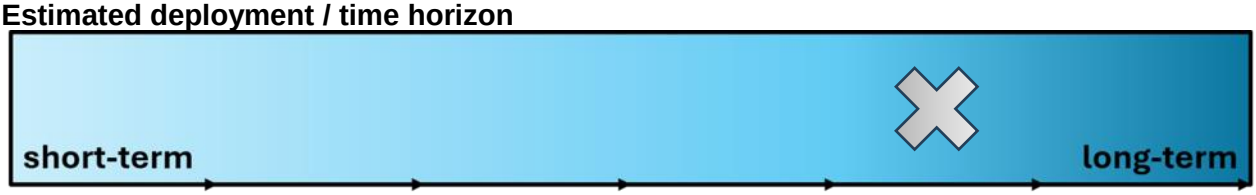


Figure 21: Recommendation Card: Business Models, Value Networks and Organisational Change

Commercial deployment and business-model innovation for automated freight

The commercial deployment of SAE Level 4 automated freight at scale requires business-model innovation across the wider logistics ecosystem. The business models of vehicle manufacturers, automation providers, logistics operators, infrastructure operators, remote-operation providers and other technology and service providers are interdependent. Decisions concerning:

- investment,
- service provision,
- data exchange,
- operational responsibility and
- risk allocation

by one actor directly affect the viability of the other actors' business models. Existing logistics contracts are often designed around variable, short-horizon cost structures such as per-kilometre rates, volume-based pricing or short notice periods, which may not accommodate the capital intensity, extended development timelines and multi-actor infrastructure dependencies that characterise SAE Level 4 freight systems.

There is no single blueprint or business model for CCAM freight. Different configurations may distribute vehicle ownership, automated-driving capabilities, remote supervision, infrastructure provision and logistics operations across different combinations of actors. These configurations are also not static: they will evolve as technology matures, regulation develops, deployment volumes increase and organisations acquire new capabilities. Business-model development should therefore be treated as a continuous process in which actors define and periodically reassess their roles, dependencies, value propositions, cost structures and risk exposure based on operational evidence and changing deployment conditions.

Investment requirements and barriers

The investment required to bring an automated freight system to commercial readiness spans:

- vehicle adaptation and type approval,
- digital and physical infrastructure co-investment,
- remote operations staffing and training,
- safety case development, and
- logistics process integration,

which is a portfolio of capital commitments that no single actor in the current value chain is individually positioned to carry [59].

Project findings show that the business case is highly sensitive to multiple factors, including:

- corridor utilisation,
- technology availability and maturity,
- regulatory clarity and road admission,
- harmonised standards,
- scalable digital infrastructure,
- workflow restructuring,
- integration requirements, and
- clear liability allocation

Given the current maturity of the technology and the information available, both upfront investment requirements and return horizons remain uncertain. Expected gains from labour savings, efficiency improvements and new service models therefore need to be assessed against considerable technical, regulatory, operational and financial uncertainty [55].

The limited readiness of logistics operators and terminal managers to invest in CCAM should therefore not be attributed to one single factor. Relevant barriers include:

- uncertainty about when suitable technology will become commercially available,
- whether and under what conditions it will receive road admission,
- how it can be integrated into existing logistics operations, and
- what organisational and financial impacts it will create.

In addition, many logistics operators are currently concentrating their investment and organisational capacity on other transitions, particularly the introduction of electric vehicles, and CCAM may not yet be an immediate strategic priority.

The absence of established financial and contractual structures for sharing risks and returns across the ecosystem adds to these barriers but should be understood as one factor among several rather than as their sole or primary cause [55] [58]. New contractual instruments like long-term service agreements, pay-per-use or subscription-based automated vehicle services represent a possible response to this misalignment, by recasting the investment profile from a single-actor capital expenditure into a distributed, risk-sharing commercial relationship whose terms can be explicitly negotiated and contractually secured [45].

Allocation of remote monitoring and remote operation

The allocation of remote monitoring and remote operation provides a concrete example of this evolving ecosystem. It is not yet clear which actor will assume this role across future CCAM configurations.

In some concepts, remote-operation services are provided by the vehicle manufacturer or automation provider; in others, logistics service providers are expected to establish or procure these capabilities through a control tower. However, individual logistics service providers:

- may not yet possess the required technical and organisational capabilities,
- may not be aware of the full implications of the role, or
- may lack the fleet scale needed to operate such a service economically.

Alternative configurations could therefore include shared remote-operation centres, specialised third-party providers or services offered by automation providers. The appropriate allocation will depend on fleet scale, operational responsibility, liability, required capabilities and the commercial model, and should be monitored and reassessed as deployment experience develops.

The simultaneous need for a harmonised, authority-facing data-provision framework, one that aligns the impact-assessment information requested by permitting and regulatory authorities with a single, consistent set of required information, reflects the same logic at the interface between commercial operators and public governance. Without such a framework, each operator faces duplicated, inconsistent reporting obligations to multiple jurisdictions that multiply administrative burden without improving the quality or comparability of the underlying policy evidence.

Organisational change, tacit knowledge and future human roles

Further, the introduction of automated freight systems imposes a depth of organisational change on multiple stakeholders that is consistently underestimated in deployment planning.

Project evidence demonstrates that the efficiency and resilience of current logistics and terminal operations rest substantially on tacit knowledge:

- informal, accumulated understanding of site-specific routines,
- informal communication between drivers and terminal personnel,
- experiential judgment in coupling and docking operations, and
- the immediate physical presence of a driver as the flexible integration point for the many small decisions that arise during a transport mission [58].

When a human driver is removed from the vehicle, none of this tacit knowledge is automatically replaced. Therefore, it needs to be deliberately captured, formalised, transferred to remote operators and other relevant personnel, embedded in digital procedures and supplemented by technical

automation of tasks that were previously performed by a physically present human as a matter of routine.

At the same time, deployment planning should explicitly identify the tasks that remain with personnel and assess how these tasks affect safety, workload, required qualifications and job quality. Human roles should not be designed merely around the residual activities that technology cannot yet perform, particularly where this would create dangerous, physically demanding, highly repetitive or unattractive work. The design of future operational roles should instead prioritise safe and meaningful work, appropriate levels of responsibility and autonomy, manageable workloads, and credible training and career-development pathways. These considerations should form part of the evaluation of alternative CCAM configurations alongside technical performance and cost [55].

The transition to automated operations therefore demands a fundamental restructuring of operational workflows. The costs and timescales of this restructuring are typically absent from ex-ante business case calculations that focus on driver-cost reduction as the primary value driver [58].

Tacit knowledge transfer should be supported through peer learning, collaborative workshops, digital platforms and scenario-based process documentation, so that site-specific operational knowledge is converted into procedures, interface requirements and training content before deployment rather than after operational disruptions occur. Survey evidence gathered across the project's operating environment confirmed this pattern: while logistics operators broadly anticipated efficiency benefits from automation, key barriers identified included high investment costs and the absence of short-term return on investment visibility; and the observation that removing a manual operation does not automatically reduce headcount costs (because terminal operations continue to require on-site personnel for functions that cannot yet be automated) points to a more complex cost-benefit structure than simple driver substitution implies [58]. Deployment planning must therefore explicitly account for business-process mapping, tacit-knowledge transfer, workflow redesign and the training obligations that accompany a credible transition from manual to automated logistics operation [58][55].

Ecosystem-level value-network and business-model analysis

The third recommendation in this card addresses the distribution of value, responsibility and risk across the enterprise objects that participate in a MODI-type automated freight operation.

An ecosystem-level value-network and business-model analysis makes explicit what informal coordination and project partnership currently obscure:

- which actors generate value,
- which bear the operational and financial risks,
- which control the critical data flows,
- which provide emerging functions such as remote supervision, and
- how the benefits of automation are distributed across a chain that spans vehicle manufacturers, automation providers, logistics operators, remote-operation centres, infrastructure owners and technology providers.

Such an analysis should not be understood as producing a single definitive CCAM business-model blueprint. It should compare alternative ecosystem configurations, clarify the dependencies between the participating actors' business models and examine how roles, value flows and contractual relationships may evolve through different stages of deployment. Continuous monitoring and

evaluation are needed because changes in technology maturity, regulation, scale and operational experience may alter which actor is best placed to perform a function or bear a particular risk.

Project evidence indicates that a value framework should identify:

- the enterprise actors involved,
- the value flows between them,
- partnerships required for resources and activities needed to orchestrate operations,
- the responsibilities attached to monitoring and compliance,
- the vulnerability and risk points created by cybersecurity, cross-border legal uncertainty and
- the data dependency, and the data needed for evaluation and quality control through harmonised schemas, KPIs and reporting processes [Annex II: Enterprise View on MODI Concept] [45].

This work should account for business viability requirements and build on the MODI findings on future business models transitions that are expected to emerge in response to SAE Level 4 CCAM freight opportunities [45]. It could also consider how logistics actors can organise and coordinate Deployment Cycle activities around freight flows that are suitable for *productive* automation, and/or how together they can redesign logistics systems around automated vehicles [45] [55].

Without the clarity that such accounts provide, deployment negotiations default to bilateral arrangements between individual partners that optimise local positions rather than system-wide value creation [45] [54]. MODI experience with collaboration models for traffic and logistics management confirmed that the highest-potential forms of cross-actor coordination require explicit governance agreements, contractual clarity on responsibilities and shared KPI frameworks – and that the absence of these structures forces actors to remain at lower, information-exchange-only levels of collaboration regardless of the technical capacity for deeper integration [54].

RC-L4-7	Trust, Public Acceptance and Human-Centred Communication												
Stakeholder	***AVO***	***AVU***	***CB***	***DIA***	***DSP***	***PIA***	***PIO***	***RO***	***SSP***	***TSP***	***TSU***	***VM***	***SIR***

Main Challenges Addressed:

- Limited explicit attention to public trust, perceived controllability, transparency/explainability and societal acceptance in the current recommendation set
- Risk of mis-calibrated trust (distrust or overreliance), and technical safety and societal trust maturing at different paces
- Lack of external HMI and standardised communication with surrounding road users in mixed traffic
- No living, lifecycle safety case explicitly covering human-factors performance, cybersecurity events and organisational governance

Recommendations

- L4-20 — Address trust, perceived controllability, transparency and explainability, and societal acceptance explicitly as deployment requirements for L4 freight, treating trust as a dynamic relationship that must be calibrated (avoiding both distrust and overreliance) rather than maximised, and translating these trust-related principles into measurable, verifiable acceptance criteria – including behavioural predictability, public interpretability and perceived operational stability – that complement technical safety evidence in approval and certification.
- L4-21 — Ensure conservative, predictable and socially interpretable driving behaviour for heavy automated freight vehicles in mixed traffic – including early signalling, stable lane positioning and conservative gap acceptance – and support it with external HMI and standardised external communication protocols towards surrounding road users, validated through measurable behavioural performance benchmarks and behavioural-consistency assessments across jurisdictions.
- L4-22 — Maintain a continuously updated ("living") safety case across the full operational lifecycle – covering technical assurance, operational learning, human-factors performance, cybersecurity events and organisational governance, and reflecting over-the-air updates – supported by documented periodic safety reviews, mandatory safety-critical incident reporting, traceable corrective actions and independent audits, so that operational data and human-oversight metrics feed continuously into risk assessment and approval renewal.

Estimated deployment / time horizon

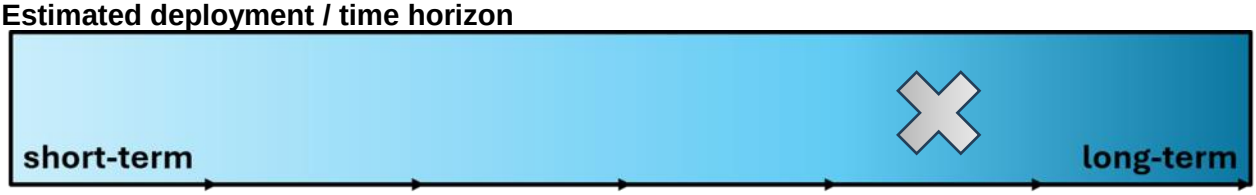


Figure 22: Recommendation Card: Trust, Public Acceptance and Human-Centred Communication

Societal acceptance and trust calibration

Technical capability alone is insufficient for the large-scale deployment of SAE Level 4 automated freight transport. Societal acceptance depends not only on whether a system is safe in the engineering sense, but on whether it is perceived as safe, understandable, accountable and worthy of public confidence by the people who share road space with it, who work alongside it, and who are governed by the regulatory systems that authorise its operation (Annex III).

Within the MODI project, demonstrations involving large automated freight vehicles in public traffic environments consistently showed that technical safety performance and societal trust do not mature

at the same pace: observers and road users form impressions of system stability and predictability through behavioural cues, i.e. the way a vehicle responds to unexpected situations, how it signals its intentions, whether its responses feel proportionate and legible, rather than through access to the safety data and engineering specifications on which formal approval rests (Annex III). Simulated emergency braking events during demonstration activities illustrated this precisely: even when the automated system responded correctly, abrupt vehicle responses were interpreted by nearby observers as signs of instability rather than of effective safety performance, a finding that points to the insufficiency of technical safety metrics alone as evidence of deployment readiness (Annex III).

Translating trust-related principles into measurable and verifiable acceptance criteria (alongside the technical safety evidence that certification currently requires) is therefore not a supplementary consideration but a structurally necessary extension of the approval framework for systems that operate in shared public environments [Annex III][59]. These criteria must encompass behavioural predictability, public interpretability and perceived operational stability as explicit deployment requirements and must reflect an understanding of trust not as a binary state to be achieved and fixed, but as a dynamic and continuously evolving relationship between automated systems, the organisations that operate them, and the people who interact with them across the full operational lifecycle (Annex III).

Crucially, trust must be properly calibrated rather than simply maximised: overreliance represents an operational safety risk of comparable gravity to distrust, as demonstrated during remote supervision exercises where operators who had become accustomed to stable motorway operation responded more slowly when unexpected events required rapid intervention (Annex III). Certification frameworks must therefore incorporate requirements for human oversight capability, operator engagement monitoring and clear allocation of responsibility between automation and remote personnel, not only at the point of initial approval but as ongoing operational obligations (Annex III).

Vehicle behaviour and lifecycle trust maintenance

The behaviour of the automated vehicle in the road environment is the primary interface through which public trust is formed or lost. For heavy automated freight vehicles operating in mixed traffic, predictable, conservative and socially interpretable driving behaviour is an important condition of public acceptance, because other road users cannot access the vehicle's internal system state and must rely entirely on observable behaviour to form expectations about what the vehicle will do next (Annex III).

The absence of a human driver creates a specific public communication gap that conventional vehicle design does not address: a driverless heavy freight vehicle has no facial expression, no hand gesture, no eye contact and no voice through which to resolve ambiguous interactions with pedestrians, cyclists or other drivers [Annex III][56].

External human-machine interfaces and standardised external communication protocols (visual signals, illuminated displays, acoustic interfaces through which customs officers or police can establish voice contact with remote operators) address this gap and are an important design requirement for vehicles operating in complex, shared environments (Annex III). These behavioural standards should be demonstrated through measurable behavioural performance benchmarks, validated under representative traffic conditions, and assessed for consistency across jurisdictions to support harmonised public expectations along cross-border corridors (Annex III).

The third recommendation in this card addresses the temporal dimension of trust: the way safety assurance and public confidence must be maintained across the full operational lifecycle of a deployed SAE Level 4 freight system, not established once at the point of type approval and then assumed to hold. Automated freight vehicles are not static systems: they evolve continuously through over-the-air software updates, operational learning, infrastructure changes and ODD extensions, each of which may alter the safety envelope in ways that a one-time certification cannot anticipate (Annex III).

A continuously updated living safety case is the instrument through which this lifecycle accountability can be structured and verified (Annex III). The compliance obligations that give this instrument operational force are specific: documented periodic safety reviews, mandatory reporting of all safety-critical incidents within defined regulatory timelines, traceable corrective action processes with implementation deadlines, and annual independent audits of safety governance procedures (Annex III). Certification authorities must verify that operational data, incident trends and human oversight metrics are incorporated continuously into risk assessments and renewal of operational approvals, so that authorisation is not a terminal event but an ongoing relationship between regulator, operator and system that reflects the accumulating operational evidence on which public trust depends (Annex III). This approach connects directly to the safety case framework introduced in RC-L4-2, the remote-operator competency obligations addressed in RC-L4-3, and the scenario-based validation and requirements traceability discussed in RC-L4-5.

5.4 Standardisation

Standardisation is a structural prerequisite for the interoperability, scalability, and mutual recognition of safety evidence that European-scale SAE Level 4 automated freight deployment requires. The eight recommendation cards in this chapter address standardisation needs across the following domains: shared taxonomies and assessment methods; V2X and C-ITS communication; maps and positioning data supporting automated freight corridors; vehicle – infrastructure and traffic-regulation interfaces; remote operation and cross-border interfaces; logistics, terminal, and charging process standards; the broader interoperability landscape; and the enterprise model and agreement frameworks that support cross-actor coordination at the governance level. Ways to ensure MODI recommendations on standardization are implemented into standardization processes are available [2].

RC-St-1	Taxonomies and Assessment Methods												
Stakeholder	AVO	AVU	CB	DIA	DSP	PIA	PIO	RO	SSP	TSP	TSU	VM	SIR

Main Challenges Addressed:

- Inconsistent safety, ODD, KPI, disengagement and MRM taxonomies across projects and countries
- No standardised assessment methodologies, scenario libraries or pass/fail criteria

Recommendations

- St-01 — Harmonise safety, ODD, KPI, disengagement, MRM and operational-performance taxonomies across projects, countries and stakeholders.
- St-14 — Standardise assessment methodologies, including scenario libraries, pass/fail criteria, sensitivity analyses and impact-assessment indicators.

Estimated deployment / time horizon

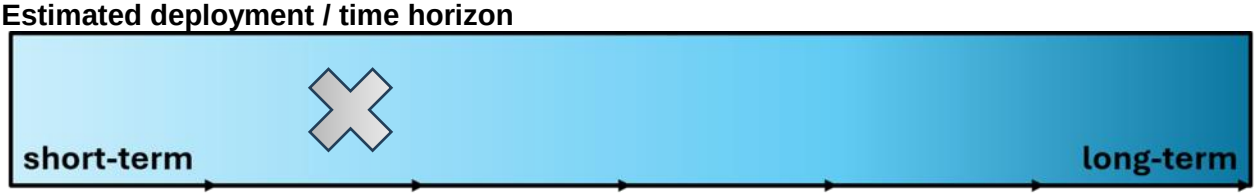


Figure 23: Recommendation Card: Taxonomies and Assessment Methods

Harmonisation and operationalisation of shared definition frameworks for SAE Level 4

The operational comparability of SAE Level 4 automated systems across projects, countries, and organisations depends, at the most fundamental level, on consistent application of the shared definitions that anchor their evaluation. Core operational terms such as ODD, MRM, disengagement event, and safety Key Performance Indicator (KPI) are not undefined: foundational frameworks exist at the international level, including SAE J3016 on driving automation taxonomy [18], ISO 34503:2023 on ODD specification [19], and the UNECE GRVA draft regulation [20], which explicitly identifies a uniform safety validation methodology as a prerequisite for cross-jurisdictional type approval [58]. However, the existence of these frameworks has not translated into consistent operationalisation across projects, national permit processes, or regulatory assessment regimes. Definitions originating from different standards bodies are only partially overlapping, and their translation into concrete testing criteria, reporting formats, and permit conditions is left largely to the discretion of individual national authorities or project consortia [58]. The consequence is that safety and performance data generated in one project or country cannot be reliably compared with findings from another; permit assessors in different national authorities apply divergent criteria to materially similar situations; and the body of evidence that would otherwise accrue cumulatively across the European SAE Level 4 development programme remains fragmented and non-transferable [52] [58]. The first recommendation of this card therefore does not call for new definitions to be invented, but for the harmonisation and coordinated operationalisation of existing frameworks.

Standardisation of assessment methodologies for comparable safety testing

The companion recommendation to standardise assessment methodologies addresses the methodological layer without which harmonised taxonomies cannot be operationalised into comparable results. Corridor assessments indicate that scenario libraries for safety-critical edge cases, underpinned by field-validated simulations, are an important tool for systematic ODD boundary-testing, for identifying infrastructure conditions that trigger degraded operational modes, and for benchmarking MRM execution across different route segments and vehicle configurations

[59]. Human-machine interface (HMI) evaluation work further supports a scenario-based approach: relevant test use cases can be derived from possible system states and mode transitions, assessed heuristically against applicable norms and best practices, and then evaluated empirically using standardised study designs and performance metrics [48]. The same evidence also cautions that higher-level pass/fail criteria, such as whether interaction is timely or effective, require explicit definition because empirical evidence is more mature for lower-level indicators than for complex human–automation cooperation outcomes [48].

Safety-testing evidence strengthens this methodological recommendation while also showing that standardisation should remain realistic about current gaps. The project developed and applied a structured assessment workflow for public-demonstration readiness from a technical-service perspective, including defined roles for assessor, applicant, and approver, but the work also found that the methodology was time-consuming and could be further narrowed and standardised for more generic application [50]. The same safety-testing evidence identifies the need for clearer guidance on how Target Operational Domain (TOD) and ODD should be specified, compared, and assessed at their boundaries, and for clearer criteria to derive a relevant and sufficient ADS test scope, including scenario coverage and the interpretation of additional relevant tests in relation to the specified ODD and TOD [50]. Without a clearly defined use case and intended operational behaviour, meaningful assessment criteria, test methods, and acceptance thresholds become difficult to define consistently [50].

Towards a unified European validation framework

The international regulatory context similarly points toward convergence on a harmonised validation framework: UNECE GRVA's draft regulation on automated driving systems identifies a uniform safety validation methodology as a prerequisite for cross-jurisdictional type approval, and the European Commission expert working group's guidelines on pre-type approval testing explicitly aim to enable mutual recognition of testing results conducted in different EU member states [20] [58]. Logistics-assessment work adds that ex-ante impact assessment should also be standardised so that different CCAM designs can be compared with current logistics operations, while current tooling focuses on cost impacts and envisages future modules for additional KPIs such as safety, efficiency, and sustainability [55]. Without agreed pass/fail criteria and shared scenario definitions, results produced by one assessment body cannot serve as the evidential basis for authorisation decisions by another, making each deployment programme effectively a standalone exercise and foreclosing the regulatory efficiency gains that a standardised European framework could deliver [58].

RC-St-2	V2X and C-ITS Communication Standards												
Stakeholder	AVO	AVU	CB	DIA	DSP	PIA	PIO	RO	SSP	TSP	TSU	VM	SIR

Main Challenges Addressed:

- Re-standardising V2X/C-ITS messages that already exist instead of closing real gaps
- Missing PKI, certificate and trust frameworks for C-ITS/V2X
- Undefined accuracy/confidence requirements for sensor-derived data in V2X containers
- Unreliable message delivery under dense, high-load V2X conditions

Recommendations

- St-02 — Build on the existing V2X and C-ITS message standards (CAM, DENM, MAPEM, SPATEM, CPM, MCM, VAM) and extend or improve them only where gaps exist – e.g. harmonised semantics, quality indicators and confidence levels – rather than re-standardising messages that are already defined.
- St-12 — Standardise PKI, certificate management and trust frameworks for C-ITS and V2X communication.
- St-20 — Define standardised accuracy, uncertainty and confidence requirements for sensor-derived data elements embedded in V2X message containers, especially where cooperative data may support safety-relevant functions.
- St-21 — Define congestion-control requirements and adaptive communication strategies for dense V2X environments to ensure reliable delivery of critical messages under high communication load.

Estimated deployment / time horizon

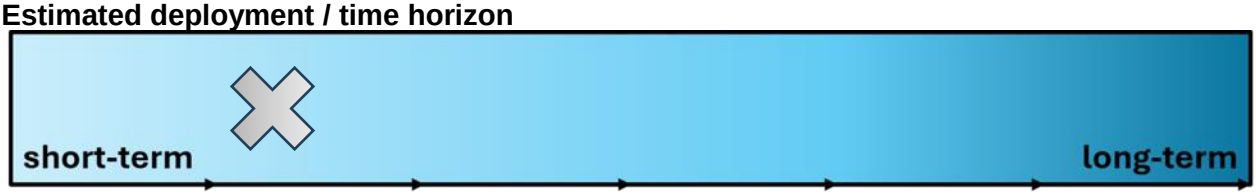


Figure 24: Recommendation Card: V2X and C-ITS Communication Standards

Existing V2X standardisation framework

The V2X and C-ITS communication layer represents the technical backbone through which automated vehicles exchange situational awareness, traffic event information, and cooperative manoeuvre intentions with roadside infrastructure and with other vehicles. A significant degree of standardisation activity has already been undertaken at the European level: the European Telecommunications Standards Institute (ETSI) [21] specifies the message types centrally relevant to automated freight operations while the C-Roads platform complements these standards by defining usage profiles, so-called Facility Layer Services, that specify how data fields within ETSI-defined messages should be populated for specific application contexts [56]. This layered standardisation architecture, in which C-Roads does not introduce new message formats but rather constrains the application of existing ETSI specifications, has proven functional in cross-manufacturer and cross-infrastructure deployments [56][52]. The first recommendation of this card therefore does not call for the re-standardisation of messages that are already defined; it calls for building on this established framework and closing specific gaps in harmonised semantics, data quality indicators, and confidence levels where the existing specifications are incomplete or inconsistently applied.

Lessons from corridor demonstrations

The demonstrations conducted along the MODI corridor from Rotterdam to Oslo produced direct evidence of both the maturity of the existing standards and the gaps that remain. MAPEM and SPATEM messages formed the basis of the GLOSA service at signalised intersections; DENM-based Road Works Warnings were successfully transmitted end-to-end from the on-site contractor through a national interchange to the vehicle; CPM-based cooperative perception was validated in Vulnerable Road User (VRU) protection and shared perception scenarios using ETSI TR 103 562; and MCM messages between vehicles supported real-time trajectory negotiation for automated cooperative merging [56] [58]. At the same time, the demonstrations identified concrete gaps. No standardised method exists for defining the quality of traffic light forecast content within SPATEM messages: the absence of this standard required a project-specific quality assessment metric to be developed ad hoc, and the resulting instability in predicted signal phase durations was identified as a trust risk for automated systems [56]. A further observation confirmed that message conformability depends on timely and synchronised software updates across all participating stations – a production vehicle with a missing update failed to transmit CAM messages correctly during an otherwise successful demonstration[58].

Extending standards

The complementary recommendations on sensor-derived data confidence (St-20) and congestion control (St-21) address two further dimensions of V2X standardisation not covered by the existing message content specifications. Demonstrations of infrastructure-based VRU detection using CPM messages revealed that object classifications produced by roadside LiDAR sensors and those produced by onboard vehicle perception systems exhibited systematic inconsistencies, reflecting differences in sensor position, calibration, and classification logic [56]. As cooperative perception systems increasingly rely on CPMs to fuse infrastructure-generated and vehicle-generated object lists, the absence of standardised accuracy, uncertainty, and confidence metadata within V2X message containers prevents receiving systems from weighting incoming data appropriately or flagging observations below safety-relevant reliability thresholds – making a common object classification schema a prerequisite for trustworthy multi-source fusion [56][50]. For high-density V2X environments, channel loading poses an additional standardisation concern: large numbers of simultaneously transmitting stations risk degrading the delivery reliability of safety-critical messages, and project evidence identifies the need for congestion-control requirements and adaptive communication strategies to address this in dense traffic conditions [52][50].

Security architecture and cross-border trust frameworks

The security architecture underpinning V2X communication constitutes a fourth and structurally foundational dimension of C-ITS standardisation, addressed by St-12.

MODI demonstrations in Hamburg confirmed that PKI certification of C-ITS messages is technically feasible at operational scale: all infrastructure-based C-ITS messages transmitted during the MODI demonstrations were PKI-certified, including CPMs generated by the roadside ITS station and forwarded to the Hamburg PKI server for signing before broadcast [56]. Connectivity and interface findings further show that message exchange for coordinated CCAM depends on reliable, secure, and interoperable communication between vehicles, roadside systems, remote-operation functions, and cloud-based services, which makes authentication and trust management part of the operational communication architecture rather than a purely back-office security function [46] [51]. Trust in

cooperatively received data, however, extends beyond the technical certification of individual messages: project findings identify cross-manufacturer trust as a broader challenge, with concerns that a vehicle system might decline to act on perception data originating from another manufacturer's vehicle or from an infrastructure source whose calibration and maintenance status cannot be independently verified [52]. The increased reliance on real-time connectivity for safety-relevant functions amplifies these concerns, requiring security and privacy architectures that are harmonised across both national PKI deployments and cross-border operational contexts [52]. Existing regulations such as UNECE Regulations 155 and 156 address certain aspects of cybersecurity and software update management [22][23], but do not fully specify the cross-border trust framework required for a multi-country corridor [52].

RC-St-3	Maps, Positioning and Corridor Data Standards												
Stakeholder	AVO	AVU	CB	DIA	DSP	PIA	PIO	RO	SSP	TSP	TSU	VM	SIR

Main Challenges Addressed:

- Fragmented map, routing and lane-level data formats with no common base model
- No European profile standards for GNSS augmentation and local positioning
- Non-standardised generation and exchange of heavy-vehicle drivable corridors

Recommendations

- St-07 — Develop a common basic road data model with standardised formats for digital maps, routing, and lane-level information to serve as an interoperable foundation across the value chain.
- St-18 — Develop European profile standards for GNSS augmentation/enhancement and non-GNSS local positioning systems used by automated vehicles, including communication profiles, accuracy/availability requirements and fusion of positioning data sources.
- St-19 — Standardise the generation and exchange of heavy-vehicle drivable corridors by specifying how routing maps, perception data, drivable-space representations, and V2X inputs are integrated into actionable corridor definitions.

Estimated deployment / time horizon

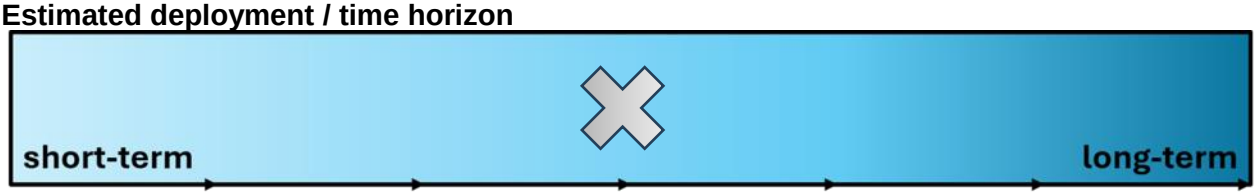


Figure 25: Recommendation Card: Maps, Positioning and Corridor Data Standards

HD maps and the need for a common road data model

Lane-level digital maps, high-accuracy positioning services, and the data formats through which these resources are generated and exchanged constitute the geospatial support layer on which automated freight operations depend for localisation, path planning, and ODD definition. HD maps complement onboard sensor systems by providing advance knowledge of lane geometry, traffic regulation, and infrastructure topology. This knowledge would enable earlier manoeuvre preparation and serves as a redundancy layer when sensor performance is degraded [52] [59].

Yet the HD map landscape remains dominated by vendor-specific proprietary formats with no common base model: road authorities, map providers, and vehicle manufacturers each hold partial datasets with differing structures, coverage levels, and update cadences, making cross-border

interoperability and systematic corridor-level assessment difficult to achieve without bespoke integration work [52].

A common basic road data model (within which existing open formats such as OpenDRIVE, Lanelet2, ADASIS, or GDF profiles can be aligned around shared content requirements, reference frames, and interface conventions) would allow all actors to retain specialised datasets while ensuring that the safety-relevant geospatial base is consistent and transferable across jurisdictions [52] [59].

Corridor evidence: value of standardised map layers

A corridor analysis illustrates both the analytical value of a standardised map layer and the consequences of current gaps. Lane-level HD map data enabled a segment-by-segment MRM feasibility assessment across the full route, which is a systematic analysis that would not have been possible without geometrically consistent lane-boundary and shoulder-width information. Variable speed limit signs, by contrast, could be detected from camera systems at only 62%, illustrating how HD map coverage linked to real-time authority data could provide essential redundancy where sensor-based recognition is unreliable [59]. These findings confirm that standardised map content requirements are a prerequisite not only for vehicle operation but for reproducible, cross-nationally comparable infrastructure readiness assessments [52] [59].

Positioning services and data harmonisation

The harmonisation of positioning services and drivable-corridor data presents parallel challenges. Empirical testing of eleven receiver–correction-service combinations along the corridor revealed a wide performance spread reflecting the absence of European profile standards specifying minimum performance requirements for GNSS augmentation services [59].

Cross-border operation is further complicated by national ETRS89 reference frame realisations that produce positional misalignments of up to 2.4 cm at border transitions, confirmed through simultaneous measurements on both sides of the border between Norway and Sweden [58]. Beyond GNSS, the generation and exchange of heavy-vehicle drivable corridors by combining routing maps, drivable-space representations, and perception outputs, equally lacks standardised methods and interfaces, making path planning and remote-support workflows dependent on provider-specific conventions rather than shared formats [50] [51].

RC-St-4	Vehicle–Infrastructure Interfaces and Traffic-Regulation Execution												
Stakeholder	AVO	AVU	CB	DIA	DSP	PIA	PIO	RO	SSP	TSP	TSU	VM	SIR

Main Challenges Addressed:

- Vehicle–infrastructure, cloud, terminal and charging interfaces not aligned with existing standards
- Machine-interpretable traffic-regulation frameworks not standardised
- No standardised interface for authorisation to enter an infrastructure authority domain and provide monitoring data
- Missing European profiles for roadside↔in-vehicle and traffic-management↔vehicle interaction

Recommendations

- St-03 — Align vehicle–infrastructure, vehicle–cloud, remote-operation, terminal, gate, charging and logistics interfaces with existing standards (e.g. ETSI), and extend or update them only where concrete gaps for automated freight are identified.
- St-11 — Standardise machine-interpretable traffic regulation frameworks, including METR-based approaches, unique identifiers and harmonised feature catalogues for traffic regulations, signs, road markings and signals.
- St-17 — Standardise the interface by which an automated vehicle, or an authorised entity acting on its behalf, requests authorisation to enter an infrastructure authority domain and provides monitoring-relevant vehicle data independent of make and model.
- St-23 — Develop a European profile standard for the applications and services exchanged between roadside (ITS Field) systems and in-vehicle (ITS Vehicle) systems, covering traffic-regulation execution, infrastructure and environmental data, and ITS services relevant to automated driving.
- St-25 — Standardise the interface between infrastructure traffic management systems and ITS Vehicle systems to enable secure, interoperable and cross-border traffic management of automated vehicles within physical-infrastructure authority domains.

Estimated deployment / time horizon

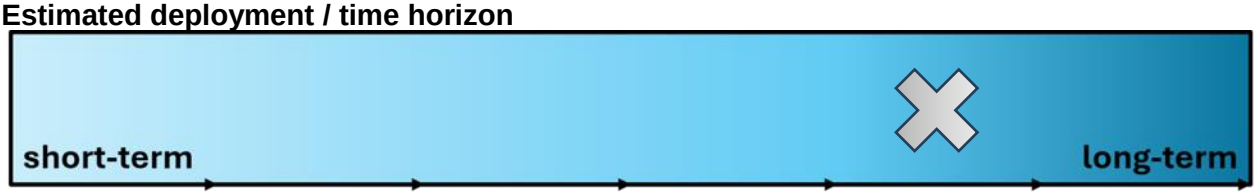


Figure 26: Recommendation Card: Vehicle–Infrastructure Interfaces and Traffic-Regulation Execution

Interface standardisation challenge: building on existing frameworks

The five recommendations grouped on this card address a single structural challenge: the application-level interfaces between automated vehicles and the broader infrastructure systems they operate within are not governed by a coherent and interoperable standards framework. This is not a case of complete standardisation absence: ETSI specifications exist for basic V2X message types, and several national implementations have demonstrated functional V2I links under project conditions.

Consequently, the resulting task is to align existing and new vehicle–infrastructure interfaces with established standards such as ETSI and to extend or update these only where concrete gaps for automated freight operations can be demonstrated, rather than treating the interface landscape as a blank slate.

MODI findings support this targeted approach: the interface landscape is explicitly differentiated into C-ITS, coordination, remote-operator communication, remote driving, OEM back-office, and dedicated support interfaces, each with different functions, data flows, and safety implications [51]. Achieving interoperability therefore requires standardisation work across four interrelated interface types: machine-interpretable traffic regulations, roadside-to-vehicle application profiles, traffic-management-to-vehicle data exchange, and authority-domain access authorisation.

Machine-interpretable traffic regulations: the most immediate need

The most operationally immediate interface standardisation needs concerns machine-interpretable traffic regulation. Field data collected along the Rotterdam–Oslo corridor showed that dynamic overhead signs constitute the most frequent and high-impact perception challenge for automated systems, particularly in the Netherlands, and that existing national databases do not capture these reliably in any common machine-interpretable format [59].

A practical pathway exists: the ISO 24315 series (METR – Management of Electronic Traffic Regulation) provides a standardisation foundation for encoding traffic regulations with unique identifiers, geometry, time validity, and lane applicability [24], and the NAPCORE project is actively merging DATEX II and TN-ITS into a unified European exchange framework that would give road authorities a common channel through which to publish regulation data [52]. Interface requirements reinforce this pathway by treating digital representation of traffic regulations as a necessary input for automated navigation and compliance, including the need for road authorities to provide regulations in machine-interpretable form that can be consumed by HD maps and vehicle systems [51].

Project findings indicate that a concrete implementation step for infrastructure operators is to establish real-time APIs for variable message signs and digital traffic sign feeds using METR-compliant data models, with associated quality assurance procedures [59].

The Norwegian Road Administration's ongoing work to convert its variable message sign data into DATEX II/METR format for distribution via national traffic management systems illustrates that this is technically feasible within existing national infrastructure arrangements and does not require a wholesale new platform [52]. European profile standards for the applications and services exchanged between roadside ITS Field systems and in-vehicle ITS Vehicle systems (the scope of St-23) would build directly on this METR and DATEX II foundation, defining what regulation, infrastructure, and environmental data must be made available to vehicles in a form that any compliant onboard system can interpret, independent of manufacturer or national origin [56].

Traffic management to vehicle data exchange: bridging public and private systems

The standardisation of the interface between infrastructure traffic management systems and automated vehicle systems (addressed by St-25) confronts a distinct challenge at the public-private boundary. MODI findings document a significant scalability gap: while local bilateral arrangements between individual confined-area operators and adjacent road authorities have proven workable in specific contexts, no standardised and scalable framework exists for private logistics operators to integrate digital traffic management capability from public orchestrators into their own TMS platforms, or to provide planning-relevant data back to those orchestrators [54].

Demonstrations and stakeholder consultations confirmed that vehicles should receive traffic management information in a standardised form as they traverse multi-country routes, such that the information content and format are consistent regardless of where along the corridor a local

operational issue arises [54]. DATEX II is identified as a candidate shared base for cross-sector data exchange, with evidence from corridor-adjacent implementations showing that the TMS-to-vehicle data pathway functions at smaller scales and could be extended to the automated freight context [54]. Realising this at the European level requires both technical standardisation and a legal and governance framework clarifying how public authorities can engage in structured digital data exchange with private logistics operators within existing regulatory constraints [54].

Authority-domain access interfaces: digital identity and permission management

The authority-domain access interface addressed by St-17 extends this same interoperability problem to the point at which an automated vehicle enters, operates within, or transitions between domains controlled by different infrastructure authorities, terminal operators, or logistics-site managers. Coordinated CCAM operation requires interfaces that can exchange strategic mission instructions, routing information, gate or area access information, and vehicle status information in a structured way, while keeping remote assistance and remote driving conceptually distinct because they carry different operational and safety responsibilities [51].

This supports the need for a make- and model-independent interface through which an automated vehicle, or an authorised entity acting on its behalf, can request permission to enter an infrastructure authority domain and provide monitoring-relevant data during operation [51]. Connectivity requirements point in the same direction by identifying the need for digital identity and access-related information for vehicles, trailers, cargo, transport orders, and permissions, so that automated freight can avoid manual checks while maintaining secure authorisation processes [46].

The standardisation task is therefore not only to define a technical API, but also to define which identity, authorisation, routing, status, and monitoring data elements must be exchanged, at what quality and latency, and under which security and governance assumptions [46] [51].

RC-St-5	Remote-Operation, Border and Enforcement Interfaces												
Stakeholder	*AVO*	*AVU*	*CB*	*DIA*	***DSP***	***PIA***	*PIO*	***RO***	***SSP***	***TSP***	*TSU*	***VM***	*SIR*

Main Challenges Addressed:

- No standardised secure interfaces for remote operation (including cargo-status access)
- Border, customs and enforcement contexts lacking secure C-ITS-based vehicle/cargo access APIs

Recommendations

- St-24 — Standardise secure and interoperable interfaces for remote operation between remote-operator personal devices or central remote-operation systems and ITS Vehicle systems, including cargo sensor interfaces where remote operators need cargo status for assistance, incident handling or monitoring.
- St-26 — Standardise CEN/ISO C-ITS-based APIs between vehicle on-board equipment and authorised roadside or personal equipment in border, customs and enforcement contexts to enable secure access to vehicle/cargo information, routing instructions and emergency or control services.

Estimated deployment / time horizon

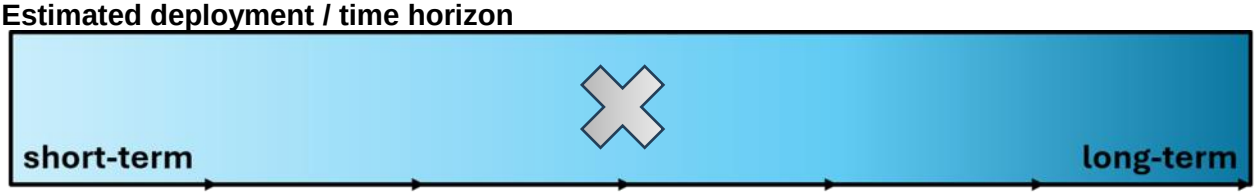


Figure 27: Recommendation Card: Remote-Operation, Border and Enforcement Interfaces

The interoperability challenge: digital interfaces for driverless border operations

When a freight vehicle has no driver, every function the driver previously performed at a border crossing or confined-area entry must be mediated through a digital interface to the vehicle's on-board equipment. Without standardised, CEN/ISO-based APIs for these interactions, proprietary manufacturer-specific solutions will emerge at each junction, creating compatibility barriers at every border transition and preventing logistics operators from sourcing remote operation services independently of the vehicle make [44]. The On-Board Equipment (OBE) of an automated vehicle has up to five external air interfaces, each a potential attack surface; the absence of a shared security architecture compounds the interoperability problem with a security fragmentation problem [44]. Both recommendations in this card address this structural gap: St-24 at the remote operation layer and St-26 at the border, customs, and enforcement layer.

Remote operation layer: open interfaces for external driving commands

The MODI border-crossing scenario established that remote driving capability is not only a safety fall-back but an operational necessity in authority-controlled contexts. When a border officer needs to move a vehicle through an unscheduled inspection lane, the vehicle's pre-planned ADS route cannot accommodate this; driving commands must be accepted from an authorised external operator on the spot [44]. The OBE–remote driver system interface must therefore be open and role-neutral: the authority to act as remote driver should be assignable to any appropriately authorised entity without vehicle-make-specific integration work [44]. Project findings also identify that no unambiguous assignment of responsibility currently governs remote driving incidents, making regulatory clarification a prerequisite alongside technical standardisation [44]. A concrete implementation pathway is available: ISO 7856 on remote support for low-speed automated driving systems provides the performance and system requirements on which a CEN profile standard for

the OBE–remote driver interface should be constructed, while the same interface architecture should extend to standardised cargo sensor data provision where remote operators require goods status for monitoring or incident handling [25] [44].

Border and enforcement layer: secure OBE interfaces for customs and inspection

The border and enforcement layer of St-26 requires standardised interfaces between the OBE and both the roadside equipment at the customs area and the customs officer's personal device. The roadside-to-OBE connection enables automated pre-selection of vehicles for inspection based on digitally exchanged vehicle and cargo data; the personal device interface supports on-the-spot officer access and should include an emergency stop capability for situations where the vehicle does not respond appropriately to obstacles [44].

Both interfaces require two-way authentication to prevent exploitation by counterfeit equipment (which is a risk heightened for vehicles carrying dangerous goods) [44]. The standardisation task is tractable: ISO 14906:2022 and EN 15509:2023 define short-range communication interfaces for electronic fee collection contexts with a directly transferable authentication architecture, while ISO 21177:2023 and the EU Certificate Policy for C-ITS deployment provide the overarching security services framework [26][27][28][29][44]. Building on these foundations rather than designing new protocols from scratch is both the efficient and the standards-compliant approach.

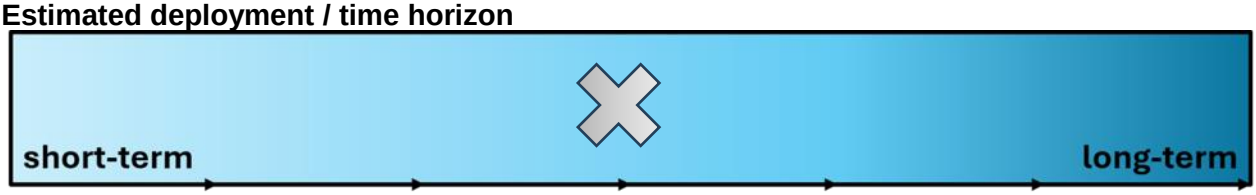
RC-St-6	Logistics, Terminal and Charging Process Standards												
Stakeholder	*AVO*	*AVU*	*CB*	*DIA*	***DSP***	***PIA***	***PIO***	*RO*	*SSP*	***TSP***	***TSU***	***VM***	*SIR*
Main Challenges Addressed: • Non-standardised logistics and terminal processes (gate access, loading, unloading, trailer/yard handling) • Fragmented automated-charging interfaces, protocols, positioning and procedures													
Recommendations • St-04 — Standardise logistics and terminal interfaces for gate access, loading, unloading, cargo handover, trailer handling and yard operations. • St-05 — Standardise automated charging, including physical interfaces, communication protocols, positioning, authentication and operational procedures.													
Estimated deployment / time horizon 													

Figure 28: Recommendation Card: Logistics, Terminal and Charging Process Standards

Digital interface gap at logistics nodes

The removal of the driver from an automated freight vehicle creates an operational gap at every logistics node the vehicle visits. Physical and communication tasks that the driver previously performed must be replaced by digital processes connecting the vehicle directly to terminal, warehouse, and yard systems. Without standardised interfaces and process definitions for these interactions, each logistics facility requires bespoke integration with each vehicle type, making the business case for automation contingent on precisely the manual interventions it was designed to eliminate [57][53].

Terminal demonstrations: gate access & loading/unloading

MODI demonstrations in the hub-to-hub use case confirmed both the technical feasibility of key terminal processes and the standardisation work they require. Gate access was validated using C-ITS messages – the system treating the terminal gate analogously to a signalised intersection, with the vehicle submitting an authenticated Signal Request Message via EU C-ITS Security Credential Management System certificates to obtain entry authorisation and loading bay routing [57]. The central finding was that a unified C-ITS standard for gate access is necessary to prevent each facility from requiring vehicle-manufacturer-specific software, reproducing at every terminal the same incompatibility that corridor deployment is designed to overcome [57]. Automated loading and unloading, demonstrated with a third-party forklift, was technically feasible but revealed that physical dock dimensions should be harmonised, manual wheel chocks replaced with automated securing mechanisms, and a common communication protocol established between vehicle systems and Warehouse or Yard Management Systems [57]. A remote operator remained essential throughout for load securing supervision and for bridging integration gaps with warehouse systems not yet equipped for automated data exchange. This confirms that full process standardisation depends on co-investment in terminal-side digital infrastructure as much as on vehicle and interface standards [57][53].

A distinction should be maintained between the standardisation of interfaces and the standardisation of processes. Logistics and terminal processes differ between sites for commercial, operational and layout-related reasons, and site operators can be expected to resist requirements that impose a uniform process model on facilities with different throughput profiles, customer structures and physical constraints. The standardisation task addressed by St-04 is therefore to define the common interfaces, message sets, data models and role definitions through which an automated vehicle interacts with terminal, warehouse and yard systems, while leaving the internal organisation of the process to the operator. A vehicle should be able to request access, receive a routing instruction, confirm a loading position and hand over cargo documentation in the same way at every node; how the node schedules, sequences and staffs the underlying operation remains a matter for the operator. Framed in this way, standardisation removes the vehicle-specific integration effort that currently arises at every logistics node without constraining the operational and commercial differentiation on which site operators depend

Automated charging processes

Further, connectivity requirements indicate that driverless charging must be treated as an integrated physical-digital process, covering vehicle positioning, charging session initiation, authentication, and back-end coordination, for which existing electric-vehicle charging standards do not fully account in the automated freight context [46] [47].

RC-St-7	Interoperability, Open Standards and the Standards Landscape												
Stakeholder	AVO	AVU	CB	DIA	DSP	PIA	PIO	RO	SSP	TSP	TSU	VM	SIR

Main Challenges Addressed:

- Lack of interoperability across OEMs, providers, maps, logistics systems and countries before scaling
- Incompatible automation environments between public roads and confined areas
- Proprietary, project-specific solutions instead of open, updateable standards
- CCAM standardisation not mapped against the existing ETSI/ISO/SAE/UNECE/CEN/NAPCORE landscape

Recommendations

- St-06 — Aim for interoperability across OEMs, infrastructure providers, map providers, logistics systems and countries before large-scale deployment.
- St-08 — Harmonise standards for public roads and private/confined logistics areas to avoid incompatible automation environments.
- St-09 — Avoid proprietary, project-specific solutions and favour open, vendor-independent, modular and updateable standards.
- St-10 — Map, compare and align CCAM deployment with relevant ETSI, ISO, SAE, UNECE, CEN and NAPCORE standards and initiatives, including their scope, location methods, road data models, feature catalogues, APIs and maintenance status.

Estimated deployment / time horizon

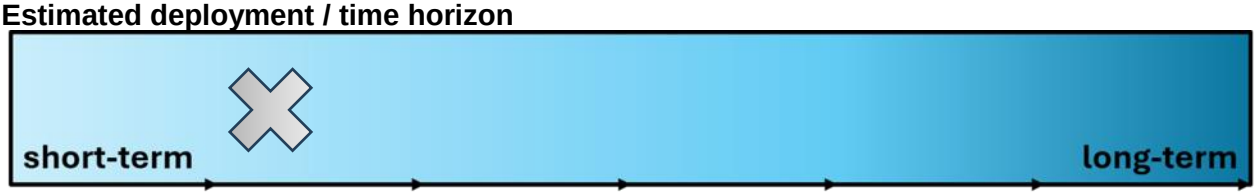


Figure 29: Recommendation Card: Interoperability, Open Standards and the Standards Landscape

Interoperability as a system-level prerequisite for corridor-scale deployment

The preceding cards of this chapter address specific technical domains, but each individual standard delivers its operational value only within a larger interoperable system. The MODI corridor spans five countries, multiple infrastructure authority domains, and dozens of logistics sites operating under different ownership and management regimes.

A vehicle that is technically compliant with only one specific proprietary interface cannot function as a corridor-scale operational asset. Project findings confirm that the benefits of C-ITS systems arise in multi-domain implementation and that the development roadmaps of vehicle and infrastructure systems must therefore be aligned. For heavy-duty freight operators active at the international level, interoperability and standardisation are the enabling conditions for collaborative traffic and logistics management schemes to function across organisational boundaries [54]. Requiring demonstrated interoperability before large-scale deployment is the practical consequence of this finding. [53]

CCAM interface architecture and the open-standards principle

The need for interoperability is reinforced by the coordinated CCAM interface architecture, which separates the interface landscape into distinct but connected parts for C-ITS communication, coordination, remote-operator communication, remote driving, OEM back-office functions, and dedicated support services such as HD maps or charging systems [51]. This architecture shows that interoperability cannot be reduced to a single V2X message set. It also confirms that existing

standardisation is uneven across multiple domains. Public-road C-ITS is comparatively mature, while remote-operation and coordination interfaces remain less standardised and are often application-specific, making them difficult to scale across the range of MODI use cases [51]. This supports the open-standards principle behind St-09: where standards already exist, they should be reused; where they are missing or too narrow, extensions should be modular, vendor-independent, and aligned with the wider standards landscape rather than implemented as proprietary project-specific solutions [51].

Public-private continuity: harmonising interfaces across road and confined-area boundaries

A specific interoperability gap arises at the boundary between public roads and confined logistics areas. An automated vehicle does not change its technical architecture when it drives from a motorway into a terminal; it should not encounter an incompatible control environment when it does so. Project evidence demonstrates that this continuity is achievable: confined area physical and digital infrastructure (PDI) designed explicitly around the principle of being "interoperable with any automated truck and applicable as an open standard for any confined area" has been validated in field tests, and the application of standard C-ITS messages within the confined area control architecture proved technically effective [53]. Connectivity requirements similarly treat MODI use cases across public roads, confined areas, gates, terminals, charging locations, ports, and motorway transitions as part of one operational connectivity problem rather than as isolated technical domains [46]. Harmonising these frameworks is a precondition for the seamless public-private operational continuity the corridor concept requires [53]. The vendor-independence and modularity principle (St-09) follows directly: a confined area PDI architecture designed around open, scalable, and vendor-independent standards allows any compliant vehicle from any manufacturer to operate on any compliant site, whereas proprietary implementations reproduce the fragmentation at the facility level that harmonised standards at the system level are intended to prevent [53].

Managing standards landscape complexity

The CCAM standardisation landscape is itself a source of complexity that must be actively managed. Across the domains addressed by this chapter alone, relevant standards and regulations are maintained by organisations such as ETSI, ISO, SAE, UNECE and CEN, while complementary implementation frameworks, specifications and deployment guidance are developed through European initiatives and stakeholder forums including C-Roads, NAPCORE and the Open AutoDrive Forum. These activities exhibit partially overlapping scopes and, in some cases, differing technical specifications for similar functional requirements [56][52]. A structured mapping and comparison of relevant standards and covering their scope, location methods, etc. is therefore a practical prerequisite for coherent implementation choices, and for ensuring that CCAM deployment builds on the most current and maintained specifications rather than on superseded or regionally limited ones [56].

From mapping to implementation: testing interoperability at the operational chain level

This mapping should guide implementation decisions before systems are deployed. The corridor evidence shows that interoperability failures emerge not only where standards are absent, but also where different actors implement partially overlapping standards, profiles, or proprietary interfaces without a shared reference architecture [51] [56]. For this reason, interoperability should be tested at the level of operational chains: a vehicle should be able to receive infrastructure and traffic-management information, transition from public road to confined area, authenticate at a gate, access

site-specific mission instructions, and exchange status with remote-operation or fleet-management systems, without requiring bespoke integration at each step [51][53][54]. The recommendation to map, compare, and align CCAM deployment with the existing standards landscape is therefore inseparable from the recommendation to require interoperability across OEMs, infrastructure providers, map providers, logistics systems, and countries before large-scale deployment. Without this system-level discipline, individual standards may be technically valid but operationally insufficient, because each would solve only a local interface problem while leaving the corridor-scale deployment chain fragmented [51].

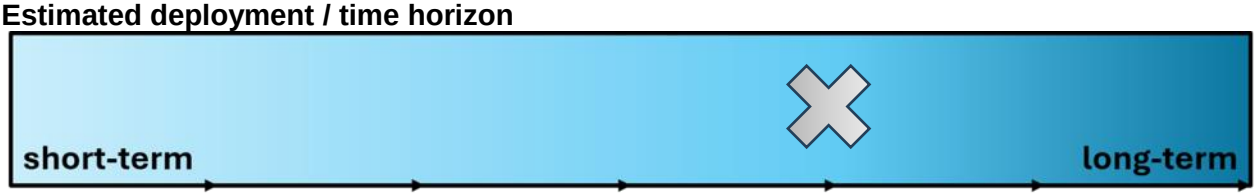
RC-St-8	Enterprise Model and Agreement Frameworks												
Stakeholder	***AVO***	***AVU***	***CB***	***DIA***	***DSP***	***PIA***	***PIO***	***RO***	***SSP***	***TSP***	***TSU***	***VM***	***SIR***
Main Challenges Addressed: • No common terminology and roles-and-responsibilities model across countries and use cases • Fragmented bilateral arrangements instead of a scalable European interaction model • Inconsistent agreements and service quality between European actors													
Recommendations • St-15 — Use the Enterprise View on the MODI concept (the MODI roles-and-responsibilities model) for MODI-like concept architectures to establish common terminology, shared responsibilities and implementation flexibility across countries and use cases and standardise the relationships between enterprise objects as far as possible to support safety, security, interoperability, scalability and a European 1-to-all interaction model instead of fragmented bilateral arrangements. • St-16 — Establish a common agreement framework for enterprise objects involved in MODI-like SAE Level 4 CCAM operations and standardise agreements as far as possible or base them on common templates to support equal treatment and consistent service quality across European actors.												
Estimated deployment / time horizon 													

Figure 30: Recommendation Card: Enterprise Model and Agreement Frameworks

The governance challenge: from bilateral to shared organisational frameworks

Technical standardisation governs how systems communicate; the enterprise model governs how the organisations behind those systems relate to one another. For MODI-like L4 CCAM concepts operating across multiple countries, operator types, and legal jurisdictions, the absence of a shared organisational framework creates the same scalability problem at the governance level that the absence of interoperable technical standards creates at the system level. A 1:1 bilateral relationship between every pair of enterprise objects involved in European-scale automated freight operations is structurally unrealistic: the number of required bilateral agreements grows combinatorially with the number of actors, and the content of each would have to be renegotiated for every new country, corridor, or use case configuration [Annex II: Enterprise View on MODI Concept].

A one-to-all relationship model – in which all actors operating within a MODI-like concept share a common organisational framework, common terminology, and common definitions of responsibilities

– is identified as the only viable path toward effective, safe, secure, and reliable corridor-scale deployment [Annex II: Enterprise View on MODI Concept]. The MODI Enterprise View proposes precisely such a model, grounded in the ARC-IT architecture framework used in ISO TC 204 ITS architecture documents, and defining twelve enterprise objects whose roles, responsibilities, and mutual expectations constitute a reusable reference architecture for MODI-like concepts[4] [Annex II: Enterprise View on MODI Concept].

Enterprise objects: functional roles vs. legal entities

The twelve enterprise objects are defined with non-overlapping responsibilities while explicitly allowing a single legal entity to fulfil multiple roles. This distinction between the functional role and the legal entity filling it provides the implementation flexibility required across countries and use cases: the same enterprise model can describe a configuration where a vehicle manufacturer also acts as remote operator, and equally one where these are independent certified third parties. Project evidence illustrates the practical value of this shared terminology: the fleet and traffic management work identified that different MODI deliverables used different names for functionally equivalent roles – confined area operator versus terminal operator, logistics management system versus TMS – with the Enterprise View providing the definitional common ground that cross-deliverable and cross-partner coordination requires [54].

Agreement framework: standardising contractual relationships across the corridor

The agreement framework proposed for these enterprise objects addresses the contractual layer that technical standards alone cannot resolve. Two fundamental relationship types structure the model: *expectation relationships*, which specify the information and services each enterprise object relies on from others, and *contractual relationships*, which formalise the obligations that govern these exchanges. The agreement framework identifies distinct agreement categories each tailored to the specific accountability structure of the enterprise object pair it governs. The core recommendation is that these agreements should, as far as possible, be standardised at the European level or at a minimum based on common templates, so that any actor capable of fulfilling a given enterprise role can enter the framework on equal terms regardless of national origin, ensuring both equal treatment and a consistent baseline of service quality across the corridor. [Annex II: Enterprise View on MODI Concept]

5.5 International, European and National Regulations

Regulatory frameworks applicable to SAE Level 4 automated freight transport are currently under active development across international, European, and national levels. Existing legal structures were designed primarily for driver-operated vehicles and have not yet been comprehensively adapted to the operational characteristics of driverless, remotely supervised systems operating across multiple national jurisdictions within a single freight mission. The five recommendation cards in this chapter address these open fields. The orientation of the recommendations is pragmatic: rather than advocating the wholesale replacement of existing frameworks, they call for targeted adaptations that extend and align current regulation to accommodate the specific requirements of SAE Level 4 automated freight operations.

Existing European instruments already provide a partial basis for extending the obligations of road authorities in this direction. The ITS Directive and its delegated regulations, for instance, already require authorities to make certain categories of road, traffic and regulatory data available through the National Access Points [12]. A similar mechanism could offer one possible route towards a

clearer and more predictable mandate for road authorities in the context of automated freight, without this deliverable prejudging which specific instrument would be most appropriate.

RC-Re-1	Approval and Permit Frameworks												
Stakeholder	***AVO***	*AVU*	***CB***	***DIA***	*DSP*	***PIA***	*PIO*	*RO*	*SSP*	***TSP***	*TSU*	***VM***	*SIR*

Main Challenges Addressed:

- Vehicle-only approval models that do not certify the operational system
- Overly static, geography-bound approvals that cannot transfer to comparable areas
- Fragmented national permit processes and duplicated assessments
- No mechanisms for continuous monitoring, permit adaptation or revocation

Recommendations

- Re-02 — Move towards corridor-, route- or service-based approval models that certify the operational system, not only the vehicle.
- Re-04 — Use performance-based approval criteria that allow approvals to be transferred to comparable operating areas (e.g. extending a campus or road-section approval to similar environments), moving beyond overly static geographical restrictions where sufficient safety evidence is available.
- Re-07 — Harmonise permit processes across Europe for automated freight trials and deployment – including parallel applications and mutual recognition between member states of safety assessments – so that Member States build on each other's results rather than starting from scratch.
- Re-14 — Create regulatory mechanisms for continuous operational monitoring, permit adaptation and permit revocation in case of non-compliance or degraded safety performance.

Estimated deployment / time horizon

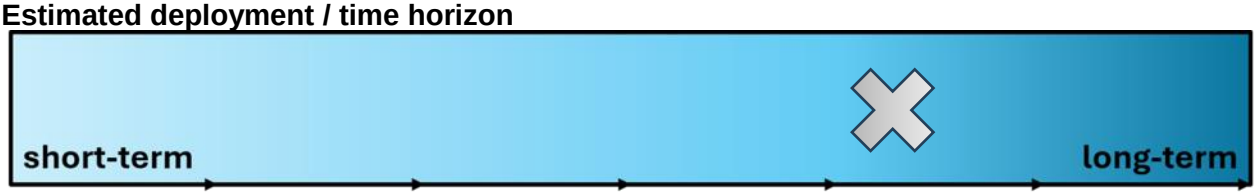


Figure 31: Recommendation Card: Approval and Permit Frameworks

From vehicle-centric to system-level approval

Current regulatory frameworks for automated vehicles were designed primarily around vehicle-level certification. For SAE Level 4 automated freight operations spanning multi-jurisdictional logistics corridors, this vehicle-centric paradigm needs to be extended: operational safety at SAE Level 4 depends not only on the intrinsic capabilities of the automated driving system but on its interaction with the physical and digital infrastructure, the precise definition and validation of the ODD, and the continuous availability of remote operation support along the route [59][58]. MODI corridor assessments confirm that a uniform SAE Level 4 claim across an entire route cannot be sustained on current evidence since safety assurance at SAE Level 4 is achievable only for specific, validated segments operating under defined conditions [59]. This empirical finding points toward the need for approval models that certify the operational system as an integrated whole, encompassing the vehicle, the infrastructure it operates within, and the governance structures that support it [58][56].

Performance-based approval models: transferable criteria for comparable operating conditions

Approvals tied to static geographical boundaries create a structural mismatch between the flexibility demanded by commercial freight logistics and the conditions under which safety has been validated. Project evidence indicates that overly conservative, geography-bound restrictions depress asset utilisation and weaken business viability, particularly where conditions on comparable route segments are functionally equivalent to those already subject to assessment. A performance-based approval model, conditioned on validated KPIs (including ODD compliance, infrastructure quality metrics, connectivity availability, positioning reliability, remote-management capability, and operator-facing interface performance) would allow operators to extend authorisations to comparable operating areas, such as applying a validated road-section approval to a functionally equivalent segment, without repeating the full permitting procedure [59][48]. Such criteria should also account for the ability of the vehicle and its supporting systems to receive operator input for functions such as route replanning, activation decisions, remote assistance, and cargo-related control where these are part of the operational concept [48].

Vehicle-level automation requirements support a section-by-section logic by linking automation readiness to defined operational conditions, technical robustness, scalability, and the availability of supporting digital systems, rather than treating L4 capability as a route-wide attribute detached from the operating environment [47]. Critically, performance-based approval must be grounded in genuinely transferable criteria, so that the safety case demonstrated for one environment can be assessed for applicability to a comparable environment through a defined recognition procedure rather than a de novo process [58].

Evidence of regulatory fragmentation: the Sweden-Norway cross-border trial

The most concrete empirical evidence for the costs of regulatory fragmentation is provided by the MODI cross-border trial between Sweden and Norway, for which obtaining the required trial permits entailed a process of nearly three years [58]. While both national frameworks proved broadly aligned in their underlying safety philosophy and documentation expectations, procedural differences introduced compounding complexity: divergent roles assigned to local and regional authorities, differing requirements for third-party technical assessment, distinct legal bases for traffic safety measures such as variable message signs and buffer vehicles, and the absence of any formal mechanism for mutual recognition of prior safety assessments [58]. At the level of permanent commercial deployment, this duplication of assessment effort is operationally and economically prohibitive. Harmonisation activities at European level constitute meaningful progress but remain limited to trial and testing contexts and have not yet been extended to permanent operational deployment [58].

Continuous monitoring and dynamic permit adaptation

Static approval provides no feedback mechanism through which real-world operational data can inform permit conditions on a continuing basis. Corridor assessments conducted within MODI demonstrate that the infrastructure-level conditions underpinning ODD validity are dynamic and can change in ways that materially affect the safety-relevance of previously approved operational parameters [59]. Regulatory mechanisms for continuous operational monitoring, built on standardised performance reporting and live quality indicators, are accordingly relevant not only to verify ongoing compliance but to generate the evidentiary basis for permit adaptation as operational

knowledge accumulates [58] [59]. The Enterprise View developed within the project identifies the obligation of physical and digital infrastructure operators to provide operational reports to their respective authorities as a critical governance mechanism, enabling authorities to detect degradation in infrastructure performance and respond with corresponding adjustments to permit conditions. Symmetrically, permit revocation procedures are necessary to ensure that the approval framework retains its safety function across the full operational lifecycle, establishing accountability for sustained compliance rather than treating initial authorisation as a one-time procedural gate whose conditions need not be revisited [58].

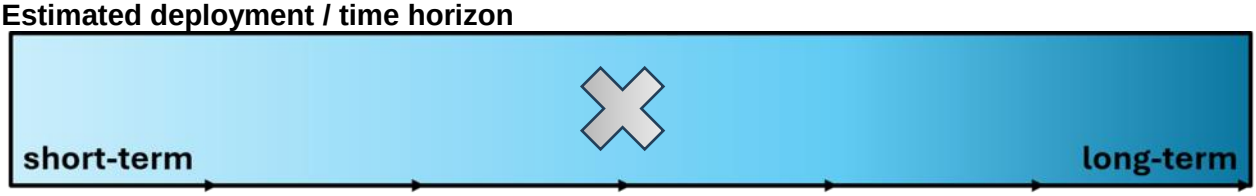
RC-Re-2	Liability and Legal Responsibility											
Stakeholder	***AVO***	***AVU***	***CB***	***DIA***	***DSP***	***PIA***	***PIO***	***RO***	***SSP***	***TSP***	***TSU***	***VM***	***SIR***
Main Challenges Addressed: • Unclear allocation of liability – distinguishing traffic-safety from cargo/goods liability – across the many actors • Undefined legal responsibility for cargo securing, vehicle condition, remote interventions and incident handling													
Recommendations • Re-03 — Clarify liability and responsibility – distinguishing traffic-safety liability from cargo/goods-related liability – between vehicle manufacturer, ADS provider, infrastructure operator, logistics operator, remote operator and cloud/service providers. • Re-10 — Clarify legal responsibility for cargo securing, vehicle condition, remote interventions, operational monitoring and incident handling.													
Estimated deployment / time horizon 													

Figure 32: Recommendation Card: Liability and Legal Responsibility

The liability gap: removing the driver as legal anchor

The removal of a professional driver from the vehicle eliminates the legal anchor around which most road transport liability frameworks are organised. Across the MODI corridor countries, existing legislation assigns responsibility for vehicle condition, cargo integrity, and incident response primarily to the physically present driver [58]. At SAE Level 4, this responsibility must be distributed across a multi-actor system including the vehicle manufacturer, ADS provider, logistics operator, infrastructure operator, remote operator, and digital service providers [Annex II: Enterprise View on MODI Concept]. MODI's enterprise architecture confirms that the actor landscape for SAE Level 4 freight is inherently multi-party and that the underlying legal frameworks which is not designed for driverless, remotely operated operations, cannot resolve the resulting liability gaps through contractual arrangements alone. In cases of identified issues (e.g. regarding safety) during automated freight operations MODI partners expect the operator to be the first contact that might need to identify the responsible stakeholder according to the contracts.

Distinguishing liability domains: traffic safety vs. cargo integrity

A fundamental prerequisite for any workable framework is the distinction between two structurally different domains: traffic-safety liability, which concerns decisions affecting the safe conduct of

automated operations and the safety of other road users, and cargo and goods liability, which concerns the condition, securing, and integrity of freight throughout the logistics chain [58]. MODI findings confirm that infrastructure operators cannot assume legal responsibility for safety-critical decisions executed by the automated driving system, as environmental variability and maintenance conditions outside their direct control make such responsibility untenable [56].

Primary accountability for safety-critical decisions rests with the vehicle manufacturer and ADS provider; however, where a remote operator provides authorised input, confirms a manoeuvre, or directly supports vehicle operation through a remote-operation interface, the liability framework must specify to which entity the resulting action is attributable [Annex II: Enterprise View on MODI Concept][51]. The certification body identified in MODI's enterprise model plays a structurally important role by formally certifying remote operators, infrastructure operators, and transport service providers against defined requirements, distributing formal accountability across the actor landscape in an auditable manner.

Unassigned operational responsibilities: cargo, vehicle condition and remote interventions

Re-10 addresses the operational responsibility domains that remain legally unassigned at SAE Level 4: cargo securing, vehicle condition verification, remote interventions, incident handling, and operational monitoring. Cargo verification at border crossings and terminals requires an identified legal actor to confirm that goods are properly secured before the vehicle resumes autonomous operation [58]. Vehicle condition compliance needs to similarly be assigned to an explicitly liable party [58]. When a remote operator acts to guide a vehicle through a customs inspection, respond to a roadside authority check, or manage an unexpected incident, the legal consequences of that action must attach to an identified entity; MODI corridor demonstrations confirmed that this question remains unresolved in practice, particularly where remote operation depends on connectivity services whose quality and availability are themselves the subject of a distinct responsibility chain [58] [44] [46].

Cross-border liability: jurisdictional challenges in transnational operations

The cross-border character of the corridor adds a further dimension: when automated vehicles and their remote operators function transnationally, the applicable jurisdiction's liability rules may remain contested. Project operations between Sweden and Norway raised unresolved questions concerning a remote operator located in one country managing a vehicle operating under another country's traffic law, with incident liability for both cargo and traffic safety remaining unclear at the time of the demonstration [58]. Existing EU-level instruments such as the Union Customs Code [30], the forthcoming Customs Reform [31], and the Product Liability Directive [32], provide partial coverage but were not designed for remotely operated, driverless freight vehicles and do not adequately address the multi-actor liability chain that SAE Level 4 logistics operations require [58].

RC-Re-3	Remote Operation Regulation												
Stakeholder	AVO	**AVU**	**CB**	**DIA**	DSP	PIA	PIO	**RO**	SSP	TSP	TSU	**VM**	SIR

Main Challenges Addressed:

- No regulatory basis for scalable operator-to-vehicle ratios
- Divergent national remote-operation rules (licensing, location, supervision, intervention authority)
- Undefined qualification, training and fitness requirements for remote operators

Recommendations

- Re-01 — Allow scalable remote-operator models, including progressive operator-to-vehicle ratios where safety and operational evidence support them.
- Re-06 — Harmonise cross-border remote-operation rules, including remote-operator licensing, location, supervision responsibilities and intervention authority.
- Re-13 — Establish clear qualification, training and fitness requirements for remote operators and operational supervisors, including mandatory operator certification, recurrent competency assessments, maximum workload thresholds and minimum communication-redundancy standards, to be demonstrated without unacceptable performance degradation during handovers, degraded-connectivity events and simultaneous alerts.

Estimated deployment / time horizon

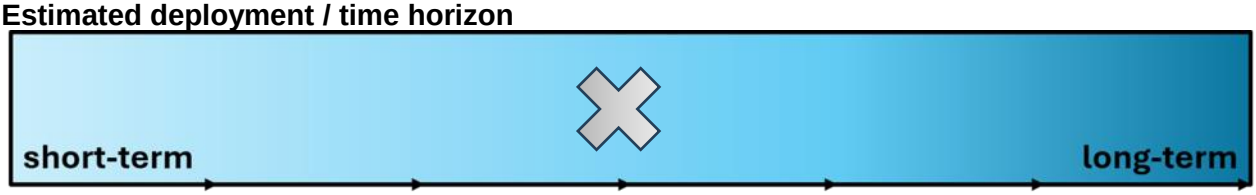


Figure 33: Recommendation Card: Remote Operation Regulation

The remote operator role: a regulatory gap in SAE Level 4 governance

The remote operator occupies a structurally novel position in SAE Level 4 freight operations: neither an on-board driver subject to standard professional licensing frameworks nor a conventional technical supervisor whose competence and accountability are defined by existing regulation. MODI demonstration experience confirms that remote operators provide strategic supervision and targeted support to the automated driving system, intervening at defined decision points, managing interactions with infrastructure and authority personnel, and assuming operational responsibility for specific actions such as cargo verification and the authorisation of vehicle movements at complex locations [57] [58]. No harmonised regulatory framework currently governs remote operator qualification, permissible supervision scope, cross-border licensing, or intervention authority, leaving a structural accountability gap at the centre of SAE Level 4 operational governance [58] [59].

Qualification and training requirements: beyond manufacturer-specific certification

On qualification and training (Re-13), project evidence indicates a consistent direction. Permit conditions for the MODI cross-border demonstration in Norway required that vehicles could only be operated by personnel who had completed manufacturer-specific training and could document this; random fitness checks for remote operations staff, equivalent to those applied to on-board drivers, were identified as a further regulatory gap [58]. This manufacturer-by-manufacturer approach cannot scale to a commercial context involving multiple vehicle types and different organisations. Operational experience further suggests that effective remote supervision requires domain-specific situational awareness – including familiarity with terminal procedures, exception handling, and

communication protocols – not substitutable by general technical competence alone, and that prior experience with the relevant category of vehicle or equipment should form part of the qualification baseline [58][48] [51]. Mandatory certification, recurrent competency assessments, defined workload thresholds, and minimum communication-redundancy standards are accordingly needed as regulatory foundations for the remote operator role [58][48] [51].

Operational viability: regulatory acceptance of multi-vehicle supervision ratios

The economic viability of SAE Level 4 automated freight services depends critically on whether regulations permit a remote operator to supervise more than one vehicle simultaneously. Project stakeholder evidence indicates that de facto expectations of a one-to-one supervision model render SAE Level 4 business models unviable at any realistic deployment scale. Scalable supervision is not purely an economic preference but an operational design problem: the acceptable operator-to-vehicle ratio depends on ODD complexity, alert frequency, connectivity reliability, and the maturity of remote-operation interfaces rather than a fixed number [55][48] [51]. Regulatory acceptance of progressive, evidence-based ratios is therefore a prerequisite for commercially sustainable SAE Level 4 operations [55].

Cross-border remote operation: harmonising licensing and intervention authority

Cross-border remote operation introduces regulatory divergence that no existing European framework addresses. MODI trial experience between Sweden and Norway showed that national authorities have not established consistent requirements for remote operator licensing, permissible location, or intervention authority across borders [58]. Swedish authorities required a valid European driving licence for operators located outside the country; Norwegian authorities accepted a European location in principle but acknowledged that the legal implications of cross-border remote oversight require further clarification [58]. Harmonised rules must cover operator licensing, permissible location, supervision responsibilities, and intervention authority so that a remote action that is technically possible and operationally necessary does not remain legally ambiguous depending on which side of the border the vehicle is on [58] [59].

RC-Re-4	Safety Assurance and Regulatory Alignment												
Stakeholder	***AVO***	*AVU*	***CB***	***DIA***	*DSP*	***PIA***	*PIO*	*RO*	*SSP*	*TSP*	*TSU*	***VM***	*SIR*

Main Challenges Addressed:

- No software-lifecycle regulation allowing updates without unnecessary full re-approval
- Risk of adding new safety-case requirements that duplicate existing regulations
- Need to align deployment with EU/UNECE/ISO frameworks and detect conflicts with national law early
- Limited acceptance of digital-first, risk-based assessment methods

Recommendations

- Re-05 — Enable software lifecycle regulation for SAE Level 4 systems, including updates, validation, monitoring and change management without unnecessary full re-approval.
- Re-08 — (Proposed) Rather than adding new safety-case requirements, align and integrate the SAE Level 4 safety-assurance recommendations with existing regulations (e.g. EU 2022/1426, UNECE R157), clarifying which actor must provide which evidence and how equivalence to a competent human driver is demonstrated.
- Re-09 — Align deployment with EU Regulation 2022/1426, UNECE Regulation No. 157, ISO 34503, ISO 26262, ISO 21448, ISO 22737, UL 4600 and related regulatory frameworks, and identify potential conflicts with national laws and regulations early.
- Re-15 — Allow digital-first and risk-based assessment methods, such as digital Site Assessment Tests, remote audits and digital-twin-supported evidence, where they provide sufficient safety assurance for SAE Level 4 CCAM trials and deployments.

Estimated deployment / time horizon

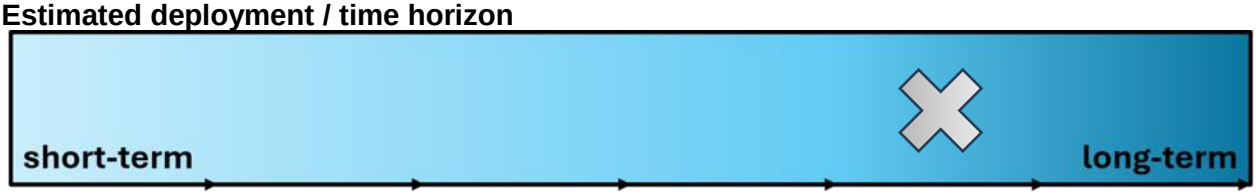


Figure 34: Recommendation Card: Safety Assurance and Regulatory Alignment

Existing regulatory frameworks: EU, UNECE, and ISO standards for SAE Level 4

A coherent normative baseline for SAE Level 4 automated freight already exists at European and international level. EU Regulation 2022/1426 constitutes the primary European type-approval instrument for fully automated vehicles [8]; UNECE Regulation No. 157, which governs Automated Lane Keeping Systems in constrained motorway conditions and represents a structural predecessor to the emerging SAE Level 4 regulatory framework [33], provides reference points for automated driving safety assurance more broadly. These instruments are complemented by ISO 26262 [34], ISO 21448 [35], ISO 34503 [37], ISO 22737 [38], and UL 4600 [36], which together define the principal functional safety, SOTIF, ODD, and system assurance requirements against which SAE Level 4 development must be measured [59]. A primary regulatory challenge for corridor deployment is not the absence of frameworks, but the incomplete mapping of how these European instruments interact with national road traffic law, working environment legislation, and port operations regulation in the individual corridor countries [58]. Potential conflicts between EU instruments and national law should therefore be identified systematically before permit applications are submitted, since MODI experience demonstrates that inconsistencies surfacing only during permitting generate compounding delays [58][44].

Safety assurance obligations: clarifying actor responsibilities

On safety assurance (Re-08), the appropriate objective is to clarify, within existing frameworks, which actor is responsible for demonstrating which aspect of safety. Permitting authorities in the MODI corridor required applicants to show that trial operations would be "at least as safe as today," with evidence covering a safety plan, system description, risk analysis with documented mitigations, and for operations relying on technical systems for traffic safety an independent assessor's report [58]. Project safety and automation requirements confirm that this evidence base must address ODD definition, hazard identification, fall-back behaviour, and operator training [43] [47]. For permanent deployment, a formally stabilised assignment of safety-case obligations across vehicle manufacturers, ADS providers, infrastructure operators, and remote operators is needed to prevent both duplication and gaps in the overall assurance chain [58][43].

Software lifecycle management: proportionate assessment of ADS updates

Software lifecycle management presents a challenge, existing type-approval frameworks were not designed to address. Current paradigms treat the approved system as a fixed artefact, yet SAE Level 4 ADS software evolves continuously through field-data integration and safety-driven corrections. A proportionate regulatory approach is needed in which updates are assessed according to their effect on the validated ODD, fall-back behaviour, and safety-relevant interfaces rather than triggering full re-approval in every case [49] [50] [58].

Assessment methods: proportionate and digital validation instruments

On assessment methods (Re-15), proportionate approaches are already emerging in practice. The Swedish Transport Agency accepted the MODI application for a new route as an extension of an existing Site Assessment Test (SAT) for the same vehicle type on a comparable operational domain, requiring no new SAT, demonstrating that authorities can calibrate assessment scope to the novelty and risk profile of the deployment [58]. Safety-testing evidence further supports a multi-pillar assurance logic combining simulation, field testing, audits, and in-service monitoring as a basis for risk-proportionate approval [50]. Digital Site Assessment Tests, remote audits, and simulation-based validation supported by digital twin infrastructure should be formally recognised as risk-equivalent evidence instruments where comparability and traceability to the validated ODD can be demonstrated [58] [50].

RC-Re-5	Data Governance and Cross-Border Procedures												
Stakeholder	AVO	AVU	CB	DIA	DSP	PIA	PIO	RO	SSP	TSP	TSU	VM	SIR

Main Challenges Addressed:

- Need for GDPR-compliant logging, monitoring and data governance across remote operation, supervision and incident investigation
- Fragmented customs, border-crossing and documentation procedures for automated freight

Recommendations

- Re-11 — Ensure GDPR-compliant logging, monitoring and data governance for remote operation, vehicle supervision, infrastructure data and incident investigation.
- Re-12 — Harmonise customs, border-crossing and documentation procedures for automated freight, including digital consignment notes and automated customs interaction.

Estimated deployment / time horizon

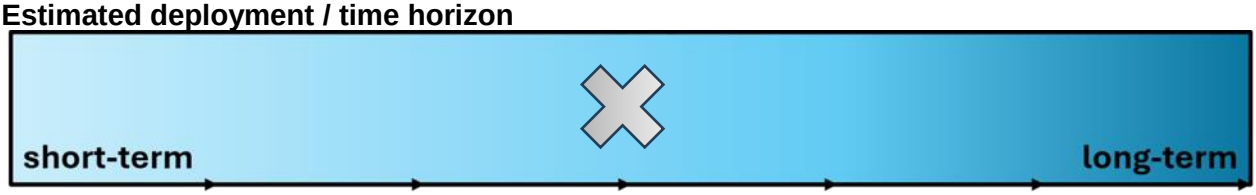


Figure 35: Recommendation Card: Data Governance and Cross-Border Procedures

Regulatory preconditions: reassigning legal responsibility for driverless border operations

Both recommendations address the regulatory preconditions for a digitised, driverless freight chain at border crossings and customs points. Existing procedures were designed around a physically present driver as document holder, point of contact with authorities, and the party legally responsible for the cargo. At SAE Level 4, none of these assumptions holds: document handling must occur through a remote operator or digital channel, and legal responsibility must be formally reassigned to a different actor by a framework that has not yet been adapted to this operational reality [58][44].

Customs and border procedures: Digitoll integration and outstanding structural gaps

On customs and border procedures (Re-12), the MODI corridor experience at the Sweden–Norway border demonstrates both the potential and the current limitations of automated customs interaction. The Norwegian Digitoll system, which enables pre-declaration of goods and automated clearance via licence-plate recognition, was successfully integrated into the demonstration, transmitting the clearance decision via C-ITS and cellular network directly to the vehicle and remote operator without requiring a stop [58]. The red-light scenario, however, exposes an unresolved gap: a CCAM vehicle directed to the inspection lane must manoeuvre in mixed traffic to a parking position while the remote operator coordinates document handling and cargo inspection with customs personnel through interfaces that do not yet exist in standardised form [58].

Outstanding structural issues include legal responsibility for goods and the misalignment between Digitoll and the forthcoming EU Customs Reform and its EU Customs Data Hub, which risks producing incompatible parallel systems unless national and European development processes are actively coordinated [58]. The eCMR protocol, in use since 2008 under a UNECE and IRU framework, provides a ready instrument for digital consignment notes [40]; the EU trust and check trader scheme offers a green-lane mechanism for CCAM operators able to meet real-time data transparency requirements [58]. Interoperable CEN APIs for the interfaces between the vehicle's on-

board equipment and customs officer devices, road authority systems, and carrier central systems form the necessary technical foundation for this regulatory environment [44].

Data governance and logging: multi-actor access, control and insurance requirements

On data governance and logging (Re-11), permit conditions for the MODI cross-border demonstration required GDPR-compliant processing of all operational and personal data [58]. D1.3 identifies the recording of information flows between the on-board equipment and the remote operator system as a requirement for operational learning and incident investigation [44]. Because remote operators, customs authorities, road authorities, OEMs, insurers, and incident investigators all hold legitimate but distinct claims to operational data, a coherent governance framework must specify not merely that data are logged, but which events trigger recording, how long data are retained, which actor controls each data category, and which parties may access it under which conditions [51][48]. Project stakeholders confirm that uncertainty over accident liability and data access is among the most significant deployment barriers identified in MODI, with insurers and regulators requiring consistent event logging standards and traceability as preconditions for the commercial insurance frameworks that SAE Level 4 operations will depend on.

6 Where to Start: Ten Priority Recommendations for Automated Freight Transport

The ninety consolidated recommendations presented in Chapter 5 were developed to address the full range of operational, technical, regulatory and governance challenges encountered across the MODI corridor and use cases. While the complete recommendation set serves as a reference for practitioners, researchers and policymakers working across the five thematic areas, a subset was identified as particularly consequential for the near- to medium-term advancement of SAE Level 4 automated freight in Europe.

At the final consortium meeting, project partners were invited to vote on the recommendations they considered most critical for large-scale deployment. The voting results served as an important input to the prioritisation process. Based on these results and the overall findings generated throughout the project, the final selection of the ten key recommendations was performed by the MODI expert team and endorsed by the Executive Board. The recommendations presented in this chapter therefore reflect both consortium-wide input and expert assessment of the measures considered most relevant for the future deployment of automated freight transport.

Unlike other MODI deliverables, this Book of Recommendations is itself a synthesis of the conclusions, lessons learned and recommendations generated across the project. Therefore, Chapter 6 serves as the concluding section of the deliverable. By prioritising ten recommendations with the highest relevance for the deployment of SAE Level 4 automated freight transport, it translates the broader set of findings presented in Chapter 5 into a practical starting point for policymakers, infrastructure providers, logistics stakeholders, industry and regulatory authorities.

Many of the recommendations presented in this chapter require investment, particularly in physical and digital infrastructure. MODI does not provide a definitive allocation of these costs to specific stakeholders, as appropriate funding arrangements depend on the investment concerned, the deployment context, existing ownership structures, the distribution of benefits and the applicable national framework. Nevertheless, the findings indicate some possible directions. Major adaptations of public physical infrastructure are generally expected to remain limited, placing greater emphasis on vehicle manufacturers developing systems capable of operating on existing infrastructure. Positioning services may require a combination of public funding and service-based revenues to ensure sufficient coverage, quality and long-term maintenance. For authoritative road and geospatial data, public funding may be appropriate where the resulting data support wider public purposes, particularly if publicly funded datasets are made broadly available for reuse. These indications should not be understood as fixed assignments of financial responsibility; the funding model should be assessed and agreed separately for each recommendation and deployment case.

6.1 Physical Infrastructure

The physical environment is the foundation on which every operational claim about automated freight ultimately rests. The two priority recommendations in this area address the two most consequential physical-infrastructure barriers identified along the Rotterdam–Oslo corridor: the absence of a shared framework for assessing corridor readiness, and the regulatory discontinuity at the boundary between public roads and confined logistics areas.

TOP 1 | PI-01 — Corridor-level infrastructure assessment criteria

"Establish CCAM-ready infrastructure assessment criteria for corridors, ports, terminals and logistics hubs, covering road geometry, lane markings, signage, maintenance and operational access conditions."

The systematic corridor assessment conducted across the Rotterdam–Oslo route revealed significant variability in the infrastructure conditions that determine whether a given road segment can be included within a defined Operational Design Domain. Lane-marking quality, sign legibility, geometric consistency, shoulder availability and operational access conditions vary considerably not only between countries but within national road networks. Without a structured assessment framework shared by infrastructure authorities, operators and vehicle developers, readiness for automated freight cannot be evaluated consistently.

This recommendation was prioritised because it addresses the gateway condition for deployment. Automated vehicles can only operate safely where the physical environment has been assessed as adequate and where that adequacy is maintained over time. A common assessment framework enables infrastructure authorities to make targeted rather than wholesale investments, gives logistics operators and vehicle developers a consistent basis for ODD definition, and creates a structured interface between vehicle-level operational requirements and the infrastructure authority's planning and maintenance obligations. For ports, terminals and logistics hubs, i.e. environments where confined-area and public-road infrastructure converge, standardised criteria also directly support the interoperability work described under Standardisation

TOP 2 | PI-12 — Alignment of public-road and confined-area infrastructure requirements

"Align public-road and confined-area infrastructure requirements to avoid operational discontinuities between public roads, ports, yards and terminals."

MODI demonstrations consistently showed that the transition between public-road and confined-area operation is currently governed by two distinct regulatory regimes that can impose conflicting requirements on the same vehicle. Road traffic legislation designed for driver-operated vehicles and the machine directives applicable in privately managed industrial areas were not developed with cross-domain automated freight in mind. A vehicle approaching a terminal gate from a public motorway encounters a change not only in physical environment but in legal framework, safety obligations and in some cases the technical requirements applicable to the automated driving function itself.

Partners prioritised this recommendation because no level of technical progress resolves a structural misalignment in regulatory frameworks. The continuity of an automated freight mission depends on continuity of the operating environment and the public-road/confined-area boundary is currently the most exposed discontinuity in that environment.

6.2 Digital Infrastructure

Digital infrastructure is the nervous system of SAE Level 4 automated freight: it carries the connectivity, regulatory data and logistics information on which the vehicle's safe and productive operation depends at every point along the route. The two priority recommendations in this area reflect the same logic — that digital services enabling automated freight must be reliable, standardised and governed by defined responsibilities, not treated as opportunistic add-ons.

A third requirement cuts across both priority recommendations rather than standing apart from them: cybersecurity. Secure digital identity, authentication and access control (DI-11, DI-12) were

highlighted during the consortium review as a dimension of comparable criticality, extending into the trust and certificate frameworks addressed under Standardisation (St-12) and the data-governance requirements addressed under Regulation (Re-11). Rather than introducing cybersecurity as an eleventh, competing priority, it is treated here as a non-negotiable property of the two Digital Infrastructure recommendations already selected: connectivity and regulatory data are only fit for safety-critical use if the channels through which they are delivered are also secure against tampering, spoofing and unauthorised access. Both priority recommendations below are therefore read, and worded, to include this requirement explicitly

TOP 1 | DI-02 — Machine-interpretable traffic regulations

"Provide traffic rules, restrictions and traffic regulations in digital, cybersecure machine-interpretable formats for automated vehicles."

Automated vehicles cannot interpret road signs the way a human driver does. They depend on digital representations of traffic regulations such as speed limits or lane restrictions, to navigate legally and safely, particularly where dynamic conditions change faster than map update cycles allow. For instance, the MODI corridor assessment identified variable overhead message signs as one of the most frequent and high-impact perception challenges for automated systems. Where sign data are not available in a structured, machine-interpretable format that the vehicle's systems can consume in near real time, the automated vehicle must rely exclusively on its onboard sensor systems to interpret regulatory information, with the reliability and latency limitations that implies.

Road authorities are uniquely positioned to provide authoritative and legally valid digital representations of the traffic regulations they establish. Such information cannot be generated reliably by vehicle manufacturers or map providers alone and is difficult to derive solely through onboard perception. As a result, road authorities play a key role in enabling machine-interpretable traffic regulations for automated driving applications.

Because automated vehicles act on this data directly, without a human driver to cross-check it against physical signage, the integrity and authenticity of machine-interpretable traffic regulations matter as much as their availability: regulatory data feeds must be protected against tampering, spoofing and unauthorised modification, consistent with the secure digital identity and authentication requirements addressed under Digital Security and Trusted Processes.

TOP 2 | DI-01 — Reliable and standardised corridor connectivity

"Ensure cybersecure, reliable and standardised connectivity – covering mobile networks, V2X communication and C-ITS services – along automated freight corridors, including interoperable inter-provider handover, network redundancy, cross-border continuity and clear responsibility for service provision."

Connectivity is a safety-critical dependency for SAE Level 4 automated freight since services such as remote supervision, safety-critical communication or connectivity-dependent positioning all rely on the continuous availability of reliable communication channels. The MODI corridor crosses five countries with different mobile network operators, different C-ITS deployment states and different regulatory frameworks governing connectivity provision. The corridor assessment confirmed that coverage gaps, handover discontinuities and the absence of defined responsibility for cross-border service quality are actual deployment barriers.

Partners assigned this recommendation the second priority in Digital Infrastructure because connectivity readiness is a precondition on which several other priority recommendations depend. Scalable remote operation, performance-based safety assessment, digital customs integration and V2X-based traffic regulation delivery all presuppose the connectivity layer.

This dependency also runs through security: a connectivity layer that is reliable but not secure would trade one deployment barrier for another, since remote supervision, V2X communication and cross-border data exchange are safety-critical functions that must be protected against interception, spoofing and unauthorised access to the same standard as the identity and access-control requirements addressed under Digital Security and Trusted Processes.

6.3 SAE Level 4 Integration in Logistics

The two priority recommendations in this area capture the operational and systemic insight that MODI's demonstrations produced most consistently: where to start, and what the actual product of automated freight deployment is. Both reflect a view of SAE Level 4 freight as a logistics system challenge, not merely a vehicle technology challenge.

TOP 1 | L4-01 — Prioritised deployment on high-volume predictable point-to-point routes

"Prioritise early SAE Level 4 freight deployment on high-volume, predictable point-to-point routes with a simple, well-defined Operational Design Domain".

Given the current state of SAE Level 4 automation technology, the operational and commercial case for SAE Level 4 automated freight is strongest where the ODD is narrow, repetitive and well-characterised. Hub-to-hub shuttle operations on motorway segments, terminal drayage corridors, and warehouse-to-warehouse short-haul routes offer the highest ratio of demonstrated performance to ODD complexity. They allow the safety case to be grounded in manageable and verifiable conditions, reduce the frequency of exception events that require remote-operator intervention, and enable the business case to be structured around predictable utilisation rather than variable demand.

This recommendation was prioritised because it captures the deployment sequence that a SAE Level 4 freight initiative should follow: identify the simplest valid ODD, demonstrate commercial viability within it, build operational knowledge and safety evidence, and expand gradually as that evidence accumulates. Attempting to deploy across the full complexity of a mixed urban–rural–motorway–cross-border corridor in a single step is technically and regulatorily difficult to deploy. A staged, ODD-led deployment strategy is the most defensible path for operators, the most tractable basis for permitting authorities, and the most legible signal to logistics markets that SAE Level 4 freight is approaching commercial readiness.

TOP 2 | L4-06 — End-to-end logistics system design

"Design automated freight vehicles as part of an end-to-end logistics system – including loading, unloading, energy/charging, documentation, scheduling and yard processes – so that the chain can operate without manual last-metre process breaks."

The most important operational insight from MODI's Swedish demonstration was about what happens at the boundaries of the driving mission. Automated loading and unloading, gate access, charging, digital documentation, and yard management are the interfaces at which an automated vehicle either creates logistics value or requires manual substitution that offsets the productivity benefit of automation. A vehicle that drives autonomously between two points but depends on

manual intervention at every logistics interface delivers a fraction of the economic and operational value that automated freight is designed to provide.

Partners ranked this recommendation second in the SAE Level 4 category because it reframes the design problem at the correct level of abstraction. The automated vehicle is not the product of SAE Level 4 freight deployment. The automated freight chain is the product. Investment in the surrounding logistics ecosystem is a prerequisite for that deployment to deliver value at commercial scale. Development programmes that treat the vehicle in isolation from logistics processes systematically underestimate both the integration costs and the value that integration unlocks.

6.4 Standardisation

Standardisation is the mechanism through which isolated technical achievements become scalable, interoperable, and commercially replicable across the diverse actor landscape of freight logistics. The two priority recommendations in this area reflect the consortium's view that the standardisation challenge for SAE Level 4 automated freight is primarily one of alignment and discipline rather than invention.

TOP 1 | St-06 — Mandatory interoperability before large-scale deployment

"Aim for interoperability across OEMs, infrastructure providers, map providers, logistics systems and countries before large-scale deployment."

A vehicle that can only operate within a proprietary interface ecosystem is not a corridor-scale asset. Interoperability is the structural condition that transforms a collection of individual project demonstrations into a scalable European deployment system. Without interoperability, each country transition, terminal access and remote-supervision handover requires bespoke integration that cannot scale.

This recommendation received the highest vote in Standardisation because it addresses a structural market condition. Requiring demonstrated interoperability before large-scale deployment is both a technical discipline and a market governance instrument: it prevents proprietary lock-in from becoming embedded at scale before a competitive, multi-supplier market can form, and it creates direct incentives for the standardisation work that is currently left to voluntary industry coordination.

TOP 2 | St-03 — Interface alignment with existing standards

"Align vehicle–infrastructure, vehicle–cloud, remote-operation, terminal, gate, charging and logistics interfaces with existing standards, and extend or update them only where concrete gaps for automated freight are identified."

The interface landscape spans C-ITS message types, remote-operation protocols, terminal access procedures, charging communications and logistics data exchange. In each of these domains, relevant international or European standards already exist. The primary standardisation task is therefore not to design new frameworks from scratch, but to systematically assess which existing standards are applicable to the automated freight context, where they require profiling or extension, and how they can be implemented consistently across countries and organisations.

6.5 International, European and National Regulations

Regulatory frameworks define the legal space within which automated freight can be authorised. The two priority recommendations in this area address the two regulatory gaps most directly

identified by MODI's corridor operations: the fragmentation of permit processes across national borders, and the unresolved allocation of liability in multi-actor automated freight chains.

TOP 1 | Re-07 — Harmonisation of European permit processes

"Harmonise permit processes across Europe for automated freight trials and deployment – including parallel applications and mutual recognition of safety assessments – so that Member States build on each other's results rather than starting from scratch."

Regulations relevant for permit processes are usually technically aligned between different national environments in its safety philosophy, but procedurally fragmented in its national implementation, with no formal mechanism for sharing safety evidence across jurisdictions. Partners gave this recommendation the highest vote in Regulation because it directly addresses one of the most concrete deployment barriers encountered in MODI. Logistics does not stop at national borders, and neither can the regulatory framework for cross-border automated freight. Harmonisation does not require identical national regulations: it requires mutual recognition of procedures, defined evidence standards and coordination mechanisms that allow a safety assessment completed in one Member State to be accepted or built upon in another. Without such mechanisms, every cross-border commercial deployment programme must incur the same compounding timeline costs for each state where the freight operation is foreseen to operate.

TOP 2 | Re-03 — Clarification of liability and legal responsibility

"Clarify liability and responsibility – distinguishing traffic-safety liability from cargo/goods-related liability – between vehicle manufacturer, ADS provider, infrastructure operator, logistics operator, remote operator and cloud/service providers."

The removal of a professional driver eliminates the legal anchor around which most road transport liability frameworks are organised. SAE Level 4 freight operations distribute the functions previously performed by a single driver across a multi-actor system without any existing legal framework having been designed to allocate responsibility across this configuration. Insurers, operators and regulators who participated in MODI confirmed that this unresolved structure is among the most significant barriers to commercial deployment: without clear liability allocation, neither insurance nor operational authorisation can be placed on a durable commercial foundation.

The fundamental distinction the recommendation introduces between traffic-safety liability, which concerns decisions affecting the safe conduct of automated operations, and cargo and goods liability, which concerns the condition and integrity of freight throughout the logistics chain is a necessary first step. The two domains involve different actors, different evidence requirements and different insurance mechanisms. Conflating them produces regulatory responses that address neither adequately, and that create inconsistent obligations for actors whose actual responsibilities lie primarily in one domain or the other.

7 References

[1] Verweij, F., Arnesen, P., Balasingam, V. (2024). Identifying potential challenges for automated driving on the route Rotterdam-Oslo from the perspective of the road operators, MODI project memo

[2] Meyer, S. F. (2025). *A strategy for implementing MODI recommendations in relevant standards*, MODI project working document (Task 1.4, TØI – Institute of Transport Economics, Norway).

[3] Regulation (EU) 2023/1804 of the European Parliament and of the Council of 13 September 2023 on the deployment of alternative fuels infrastructure. (2025, December 11). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1804

[4] Architecture Reference for Cooperative and Intelligent Transportation, https://www.arc-it.net/

[5] European Partnership on Connected, Cooperative and Automated Mobility (CCAM). https://www.ccam.eu/

[6] European Commission, *European Connected and Autonomous Vehicle Alliance (ECAVA)*. https://digital-strategy.ec.europa.eu/en/policies/vehicle-alliance, Last visited: 05 August 2026

[7] European Commission, DG MOVE, *EU Large-Scale Cross-Border Testbeds for Connected and Automated Mobility*. Connected and automated mobility | Shaping Europe's digital future, Last visited: 05 August 2026

[8] Commission Implementing Regulation (EU) 2022/1426 of 5 August 2022 laying down rules for the application of Regulation (EU) 2019/2144 as regards uniform procedures and technical specifications for the type-approval of the automated driving system (ADS) of fully automated vehicles. https://eur-lex.europa.eu/eli/reg_impl/2022/1426/oj

[9] C-Roads Platform, *Harmonised C-ITS Specifications*. https://releases.c-roads.eu/, Last visited: 05 August 2026

[10] CAR 2 CAR Communication Consortium. https://www.car-2-car.org/, Last visited: 05 August 2026

[11] NAPCORE — National Access Point Coordination Organisation for Europe. https://napcore.eu/, Last visited: 05 August 2026

[12] Directive (EU) 2023/2661 of the European Parliament and of the Council of 22 November 2023 amending Directive 2010/40/EU on the framework for the deployment of Intelligent Transport Systems. https://eur-lex.europa.eu/eli/dir/2023/2661/oj

[13] ISO/TS 24315-1:2025, ISO/TR 24315-2, ISO/TS 24315-3:2025, *Intelligent transport systems — Management of electronic traffic regulations (METR)*. https://www.iso.org/standard/87532.html

[14] ASAM e.V., *ASAM OpenDRIVE*. https://www.asam.net/standards/detail/opendrive/, Last visited: 05 August 2026

[15] Poggenhans, F. et al. (2018), *Lanelet2: A High-Definition Map Framework for the Future of Automated Driving*, IEEE ITSC 2018. https://doi.org/10.1109/ITSC.2018.8569929

[16] NDS Association, *Navigation Data Standard*. https://nds-association.org/, Last visited: 05 August 2026

[17] DATEX II (CEN/TS 16157 series), *Intelligent transport systems — DATEX II data exchange specifications for traffic management and information*. https://www.datex2.eu/, Last visited: 05 August 2026

[18] SAE J3016_202104, *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*. https://www.sae.org/standards/content/j3016_202104/

[19] ISO 34503:2023, *Road vehicles — Test scenarios for automated driving systems — Specification for operational design domain*. https://www.iso.org/standard/78952.html

[20] United Nations Economic Commission for Europe. (2025). Proposal for a new United Nations Regulation on uniform provisions concerning the approval of motor vehicles with regard to their Automated Driving Systems (Doc. No. ECE/TRANS/WP.29/GRVA/2026/3). Retrieved from https://unece.org/sites/default/files/2026-01/ECE-TRANS-WP.29-GRVA-2026-03e.pdf

[21] ETSI EN 302 637-2, *ITS; Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service*. https://www.etsi.org/standards

[22] UN Regulation No. 155 — Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system. https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security

[23] UN Regulation No. 156 — Software update and software update management system. https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update

[24] ISO/TS 24315-1:2025, ISO/TR 24315-2, ISO/TS 24315-3:2025, *Intelligent transport systems — Management of electronic traffic regulations (METR)*. https://www.iso.org/standard/87532.html

[25] ISO 7856:2025, *Intelligent transport systems — Remote support for low speed automated driving systems (RS-LSADS) — Performance requirements, system requirements and performance test procedures*. https://www.iso.org/standard/82951.html

[26] ISO 14906:2022, *Electronic fee collection — Application interface definition for dedicated short-range communication*.

[27] EN 15509:2023, *Electronic fee collection — Interoperability application profile for DSRC*.

[28] ISO 21177:2023, *Intelligent transport systems — ITS station security services for secure session establishment and authentication between trusted devices*.

[29] European Commission, *Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)*. https://cpoc.jrc.ec.europa.eu/

[30] Regulation (EU) No 952/2013 laying down the Union Customs Code. https://eur-lex.europa.eu/eli/reg/2013/952/oj

[31] European Commission (2023), *Proposal for a Regulation establishing the Union Customs Code and the European Union Customs Authority*, COM(2023) 258 final. https://taxation-customs.ec.europa.eu/customs-4/eu-customs-reform_en

[32] Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC. https://eur-lex.europa.eu/eli/dir/2024/2853/oj

[33] UN Regulation No. 157 — Uniform provisions concerning the approval of vehicles with regard to Automated Lane Keeping Systems (ALKS). https://unece.org/transport/documents/2021/03/standards/un-regulation-no-157-automated-lane-keeping-systems-alks

[34] ISO 26262:2018 (all parts), *Road vehicles — Functional safety*.

[35] ISO 21448:2022, *Road vehicles — Safety of the intended functionality (SOTIF)*.

[36] UL 4600, *Standard for Evaluation of Autonomous Products*.

[37] ISO 34503:2023, *Road vehicles — Test scenarios for automated driving systems — Specification for operational design domain*.

[38] ISO 22737:2021, *Intelligent transport systems — Low-speed automated driving (LSAD) systems for predefined routes — Performance requirements, system requirements and performance test procedures*.

[39] Tolletaten (Norwegian Customs), *Digitoll*. https://www.toll.no/en/, Last visited: 06 August 2026

[40] UNECE, *Additional Protocol to the Convention on the Contract for the International Carriage of Goods by Road (CMR) concerning the Electronic Consignment Note*, Geneva, 20 February 2008.

[41] European Commission, Directorate-General for Research and Innovation, *Call for applications – Expert group on European Union Research and Innovation for the automotive sector (EURIAS)*, 5 January 2026. https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/call-applications-expert-group-european-union-research-and-innovation-automotive-sector-eurias-2026-01-05_en. 07 August 2026

[42] Phillips, R. O., Jenserud, I., Weir, H., Liesa, F., Pernot, D., Pourmohammadzia, N., … Rostoft, M. S. (2023). *User and stakeholder requirements for automated transport in logistics* (MODI Deliverable D1.1). MODI Consortium. Sensitive – Not Published

[43] Boustedt, K., Seiniger, P., Meyer, S. F., Egner, L. E., Elvik, R., Rostoft, M. S., Roche-Cerasi, I., & Jenssen, G. (2023). *Safety and Security Requirements* (MODI Deliverable 1.2). MODI Consortium, Sensitive – Not Published

[44] Bräutigam, J., Foss, T., Jetlund, K., Brunes, M. T., Wijk, P., Rostoft, M. S., & Sirland, T. (2023). Report on Border Processes (MODI Deliverable 1.3). MODI Consortium

[45] Phillips, R., & Saghafian, M. (2026). *Future Business Models for Connected and Automated Logistics* (MODI Deliverable 1.4). MODI Consortium. Not yet published.

[46] Zhu, J., Perdok, B., Arts, G., Åberg, D., Jenssen, G, … Meijer, W. (2023). *Report on connectivity requirements* (MODI Deliverable D3.1). MODI Consortium. Sensitive – Not Published

[47] Søråsen, R., Elnes, B., Wijk, P., Schmeitz, A., Seiniger, P., Dagerhorn, U., … Moen, T. (2024). *Report on automation requirements* (MODI Deliverable D3.2). MODI Consortium. Sensitive – Not Published

[48] Wijk, P., Lindgren Walter, A., van Waterschoot, B., Jenssen, G., Moen, T., Phillips, R., … Vandenhoudt, J. (2023). *Report on user/driver-vehicle interface* (MODI Deliverable D3.3). MODI Consortium. Sensitive – Not Published

[49] Dagerhorn, U., Arts, G., Wijk, P., & Xu, W. (2025). *Adapted VOLV, DAF and EIN Vehicles* (MODI Deliverable 3.4). MODI Consortium, Sensitive – Not Published.

[50] Dagerhorn, U., Persson, J., Wijk, P., Huisman, R., Xu, W., Jenssen, G., & Lykkja, O. M. (2026). *Report on Safety Testing of Adapted Vehicles and Used Methods and Confidence Levels* (MODI Deliverable 3.6). MODI Consortium, Sensitive – Not Published.

[51] Schmeitz, A., Verhaeg, G., Foss, T., Meijer, W., Wijk, P., Huisman, R., … van der Meer, J. (2025, March 28). Validated interface for coordinated CCAM (MODI Deliverable D4.1). MODI Consortium. Sensitive – Not Published

[52] Jetlund, K., Sæther, S. R., Storrønning, T., Jakobsen, G. C., & Wold, H. (2024). *Requirements for physical and digital infrastructure (PDI) for automated freight transport* (MODI Deliverable D4.2). MODI Consortium

[53] Meijer, W., Spoelstra, J., Das, A., Schmeitz, A., & Huisman, R. (2024). *Optimal designs of physical and digital infrastructures at confined areas* (MODI Deliverable D4.3). MODI Consortium.

[54] Spoelstra, J., Mein, E., Søråsen, R., Westerheim, H., Svensk, P.-O., Briele, A., … Pöyhönen, A. (2025). *Collaborative CCAM fleet- and traffic management* (MODI Deliverable D4.4). MODI Consortium.

[55] van Kempen, E., Santing, M., van Adrichem, M., & van der Meer, J. (2025). *Methodology of logistics optimisation using CCAM* (MODI Deliverable D4.5). MODI Consortium.

[56] Johannes, T., Thelen, M., de Lange, J. W., David, H., Jelinek, R., & Wahl, R. (2026). *Demonstration Hamburg use case "Motorway to Harbour"* (MODI Deliverable D5.2). MODI Consortium.

[57] Kruse, T., Backlund, M., Wijk, P., Xu, W., Rasmussen, M. S., Värnholt, A., … Wahl, R. (2026). Demonstration of CCAM systems and services of goods transport in hub-to-hub (MODI Deliverable D5.3). MODI Consortium.

[58] Arnesen, P., Meland, S., Fagerholt, R. A., Støla, S., Sande, A. B., Mølnvik, G., … Smeds, P. (2026). *Demonstration of CCAM systems and services of goods transport on motorway and border crossings* (MODI Deliverable D5.4). MODI Consortium.

[59] Thelen, M., Sander, D., Briele, A. M., Balasingam, V., Bakke, H., Solberg, A. M., … Gualandi, E. (2026). *Assessment of CCAM-implementation along MODI-corridor* (MODI Deliverable D5.5). MODI Consortium

Annex I: Consolidated Recommendations

ID	Theme Code	Theme	Recommendation	Motivation (combined)
DI-01	DI	Digital Infrastructure	Ensure cybersecure, reliable and standardised connectivity — covering mobile networks, V2X communication and C-ITS services — along automated freight corridors, including interoperable inter-provider handover, network redundancy, cross-border continuity and clear responsibility for service provision, so that remote supervision and safety-critical communication remain available across national borders and mobile network operators.	[DI-01] The MODI corridor connects multiple countries and logistics hubs, demonstrating automated freight operations across diverse infrastructure and regulatory environments. A harmonised European approach is required to ensure interoperability and enable large -scale deployment of CCAM solutions. [DI-21] (no standalone motivation in sources — deliverable/context evidence only)
DI-02	DI	Digital Infrastructure	Provide traffic rules, restrictions and traffic regulations in digital, cybersecure machine-interpretable formats for automated vehicles.	Road authorities are the authoritative source for the regulations and must provide a digital representation of the regulations in machine - interpretable format to HD Map Traffic regulations are crucial for safe and legal navigation.
DI-03	DI	Digital Infrastructure	Establish a common lane-level digital road network as a trusted base layer for automated freight routing and operational planning.	The road network must be detailed down to lane level for automated navigation. A common digital road network can be maintained by either authorities or industry map producers but must be shared between all stakeholders.
DI-04	DI	Digital Infrastructure	Standardise HD map formats, quality requirements, governance models and frequent update and quality-assurance processes, including for confined areas such as ports and terminals as well as for temporary traffic management and construction sites.	[DI-04] Digital maps are available for public roads but not confined areas. The current SAE Level 4 vehicle concepts need some kind of HD -map. [DI-19] (no standalone motivation in sources — deliverable/context evidence only)

ID	Theme Code	Theme	Recommendation	Motivation (combined)
DI-05	DI	Digital Infrastructure	Provide dynamic road, traffic and event data — such as roadworks, closures, temporary restrictions, incidents and temporary layout changes in confined areas (e.g. relocated barriers on terminals) — in real time and machine-interpretable form.	As mobile roadworks (constantly) change their position, the RWW service of a cooperative roadworks trailer can help trucks to start their merging manoeuvre in time, although the roadworks is out of sight (e.g. behind a curve). Dynamic changes in the road network represent a particular challenge for automated vehicles.
DI-06	DI	Digital Infrastructure	Standardise infrastructure-to-vehicle real-time information (e.g. SPaT, MAP, variable message signs, traffic-sign status, rail crossings and lane status) together with the underlying API structures, data models and service-level requirements, and ensure that digital signs, VMS feeds and temporary traffic-management information from road authorities are regulated, quality-assured and provided through reliable, standardised APIs.	[DI-06] Common message formats and harmonised use case descriptions helped a lot at the interface between infrastructure and vehicle. To foster the roll out of cooperative infrastructure, C-ITS equipment should be part of the construction standard of traffic. [DI-20] (no standalone motivation in sources — deliverable/context evidence only) [St-13] Road authorities are often seen as the primary trusted source of essential data on infrastructure characteristics and road conditions. This information is important for automated vehicle decision -making and compliance with traffic regulations.
DI-07	DI	Digital Infrastructure	Standardise interfaces between automated vehicles and logistics systems, including TMS, FMS, WMS, TOS, RVOS, yard systems and control towers.	Stakeholders repeatedly stressed that autonomy only creates major value when integrated into scheduling systems, TMS/WMS platforms, charging systems, ETA management, terminals, and warehouse flows. Today, tele -ops systems and logistics TMS platforms are not harmonised, creating integration friction.

ID	Theme Code	Theme	Recommendation	Motivation (combined)
DI-08	DI	Digital Infrastructure	Integrate mission management, fleet orchestration, ETA management, remote supervision, exception handling and recovery into a coherent digital operating environment.	Stakeholders repeatedly stressed that autonomy only creates major value when integrated into scheduling systems, TMS/WMS platforms, charging systems, ETA management, terminals, and warehouse flows. A CEN API will enable an interoperable, secure, flexible, and effective Remote Operation covering both Remote Assistance and Remote Driving of automated vehicles moving around in European border areas, customs areas, harbours, terminals, and physical infrastructure for road vehicles.
DI-09	DI	Digital Infrastructure	Define data-quality, confidence, stability, latency and availability requirements for digital infrastructure services used by automated freight vehicles.	Infrastructure support for automated driving can be very helpful for automated vehicles, though the safety-critical decisions must remain in the vehicle. The Dutch use case focuses on CCAM vehicles operating in port environments, including coordination with automated guided vehicles, access control, and loading operations.
DI-10	DI	Digital Infrastructure	Apply intelligent filtering and relevance management to V2X, infrastructure and cloud data to avoid information overload and unstable system behaviour.	
DI-11	DI	Digital Infrastructure	Implement secure digital identity and cyber-secure authentication for vehicles, trailers, cargo, transport orders and access permissions, to avoid manual checks and to protect safety-critical operations against tampering and unauthorised access.	

ID	Theme Code	Theme	Recommendation	Motivation (combined)
DI-12	DI	Digital Infrastructure	Digitise gate, customs, access-control and pre-clearance processes before vehicle arrival, including support for digital documentation such as eCMR.	Business cases remain weak if autonomous vehicles still depend on local personnel for docking, gate access, paperwork, load securing, charging support, or warehouse coordination. Significant impact requires progressively automating or reorganising these surrounding processes.
DI-13	DI	Digital Infrastructure	Provide machine-interpretable information on charging availability, access, booking, pricing, connector compatibility and automated charging capabilities.	Commercial viability of SAE Level 4 freight is highly sensitive to energy cost, charging availability, and dwell time. Without interoperable charging reservation systems and transparent energy pricing integration into TMS platforms, SAE Level 4 scaling remains economically fragile.
DI-14	DI	Digital Infrastructure	Treat public digital infrastructure, including GNSS, RTK correction services, mobile networks, C-ITS services and data platforms, as core enablers of automated freight.	Positioning services must have the necessary coverage and quality (scalability, accuracy, protection, etc.) along the road networks to support automated driving. Measures to improve GNSS quality are important to gain the positive effects of C-ITS Services
DI-15	DI	Digital Infrastructure	Harmonise geodetic reference frames, map datums, elevation models, metadata and timestamps across map, positioning and C-ITS data sources.	
DI-16	DI	Digital Infrastructure	Enable seamless handover between mobile networks, RTK correction providers, connectivity technologies and national systems during cross-border operations.	
DI-17	DI	Digital Infrastructure	Use hybrid communication architectures combining ITS-G5, C-V2X, and cellular where appropriate, rather than relying on one communication technology only.	Cellular networks must have the necessary coverage along the road networks to support automated driving. Given the importance of cellular networks, the responsibility for ensuring network operators have the

				required coverage must be clarified.
ID	**Theme Code**	**Theme**	**Recommendation**	**Motivation (combined)**
DI-18	DI	Digital Infrastructure	Establish digital feedback loops between traffic management centres, road authorities, infrastructure operators and automated vehicle operators, including discrepancy reporting, data correction and quality feedback where relevant.	Structured collaboration enables alignment between infrastructure design and the operational needs of automated driving systems, which may reduce ambiguities and improve system reliability. Feedback loops can support timely, evidence-based updates to standards and guidelines as technology evolves. They also enable discrepancies and quality issues detected during operation to be reported back to the responsible actors for assessment and correction.

ID	Theme Code	Theme	Recommendation	Motivation (combined)
L4-01	L4	L4 Integration in Logistics	Prioritise early L4 freight deployment on high-volume, predictable point-to-point routes (A to B) with a simple, well-defined ODD.	Early business cases are strongest in repetitive logistics flows such as warehouse-to-warehouse shuttles, terminals, ports, drayage corridors, and future hub-to-hub long-haul operations. Stakeholders repeatedly stressed that the long-term value of L4 freight lies in public-road logistics operations rather than isolated yard automation.
L4-02	L4	L4 Integration in Logistics	Define ODD and TOD boundaries in a performance-based and graduated way rather than as binary operate/no-operate conditions.	Stakeholders reported that current ODD restrictions often create excessive downtime and low utilisation. D1.4 Business models: Current ODD constraints create significant downtime, lower utilization and business viability.
L4-03	L4	L4 Integration in Logistics	Use standardised operational-readiness frameworks covering safety cases, go/no-go criteria, risk assessment, incident response and operational approval.	MODI demonstrated that technical feasibility alone does not enable deployment; operational readiness is the real gating factor. In UC NL, integrating CCAM vehicles into live terminal and drayage environments required structured safety gates, fall-back strategies, and defined incident workflows.
L4-04	L4	L4 Integration in Logistics	Treat exception handling, recovery, fall-back operation and restart procedures as core deployment capabilities, not as secondary add-ons, and demonstrate validated degraded-mode, connectivity-loss and emergency-fall-back behaviour, since how the system behaves in these situations strongly influences public trust and acceptance.	

ID	Theme Code	Theme	Recommendation	Motivation (combined)
L4-05	L4	L4 Integration in Logistics	Develop scalable remote-supervision and remote-operation concepts, including operator roles, workload, situational awareness and intervention procedures, and define human-centred minimum requirements covering alarm prioritisation, staffing resilience, controllability, operator engagement monitoring and trust calibration to counter overreliance during stable operation.	MODI interviews identified remote-operation scalability as one of the strongest barriers to economic viability. Several stakeholders stressed that logistics operations will still require human intervention and exception management for the foreseeable future, but these roles must evolve from direct driving to scalable oversight and logistics continuity management.
L4-06	L4	L4 Integration in Logistics	Design automated freight vehicles as part of an end-to-end logistics system — including loading, unloading, energy/charging, documentation, scheduling and yard processes — and develop the wider autonomous logistics ecosystem (including automated loading, unloading and charging suppliers) so that the end-to-end chain can operate without manual last-metre process breaks.	[L4-06] Stakeholders repeatedly stressed that autonomy only creates major value when integrated into scheduling systems, TMS/WMS platforms, charging systems, ETA management, terminals, and warehouse flows. MODI evidence shows that the largest value often comes from improving the wider logistics system rather than simply replacing a driver. [L4-17] (no standalone motivation in sources — deliverable/context evidence only)
L4-07	L4	L4 Integration in Logistics	Start with simple, controlled and repeatable operational scenarios and scale gradually towards more complex environments and mixed-traffic interactions.	While confined areas are useful for reducing complexity and validating technology, they alone are unlikely to generate large-scale logistics transformation. Nevertheless, the benefits of infrastructure support are coherent, and CCAM vehicles should use the added value by infrastructure support to improve safety, efficiency and reliability of the automated driving functionality
L4-08	L4	L4 Integration in Logistics	Ensure high vehicle precision for docking, reversing, charging, coupling, loading and low-speed manoeuvring in logistics environments.	

ID	Theme Code	Theme	Recommendation	Motivation (combined)
L4-09	L4	L4 Integration in Logistics	Conduct long-term field trials under real operational, seasonal, traffic and weather conditions to validate robustness, economics and acceptance.	
L4-10	L4	L4 Integration in Logistics	Apply logistics-centred design methods and iterative V-model approaches to ensure that technical development involves alignment with logistics workflows.	
L4-11	L4	L4 Integration in Logistics	Maintain structured requirements databases linking use cases, system functions, stakeholders, infrastructure needs and validation activities.	
L4-12	L4	L4 Integration in Logistics	Include HMI and human-factors requirements for remote operators, on-site personnel and surrounding traffic participants from the beginning of system design, including external HMI for transparent communication with surrounding road users.	
L4-13	L4	L4 Integration in Logistics	Prevent remote-operator overload by designing clear alerts, prioritised information, ergonomic interfaces and appropriate task allocation.	
L4-14	L4	L4 Integration in Logistics	Use scenario-based testing and edge-case documentation — including edge cases specific to logistics integration — and complete structured closed-course, sandbox and/or simulation validation programmes before public-road deployment, covering degraded modes, remote operations, connectivity loss and emergency fall-back, independently validated against predefined thresholds and assessing both technical outcomes and human-system-interaction indicators (e.g. operator response quality and surrounding road-user interpretability).	As mobile roadworks (constantly) change their position, the RWW service of a cooperative roadworks trailer can help trucks to start their merging manoeuvre in time, although the roadworks is out of sight (e.g. behind a curve). Merging manoeuvres for large vehicles can be very complicated.

ID	Theme Code	Theme	Recommendation	Motivation (combined)
L4-15	L4	L4 Integration in Logistics	Establish a unified, harmonised data-provision framework that aligns the impact-assessment data requested by authorities (ex-ante and ex-post), so that deployment decisions can be evaluated consistently against cost, safety, productivity, sustainability and service availability while reducing duplicated reporting effort for operators.	Future deployment decisions should therefore assess system-level logistics benefits in addition to driving capability. Stakeholders repeatedly emphasised that customers ultimately care about reliable service, cost parity, and operational continuity rather than autonomy itself.
L4-16	L4	L4 Integration in Logistics	Explicitly account for business-process change, tacit operational knowledge and workflow restructuring when introducing automated freight systems.	Write three to four sentences here Write three to four sentences here Write three to four sentences here Write three to four sentences here Write three to four sentences here
L4-18	L4	L4 Integration in Logistics	Develop a value network for the enterprise objects involved in a MODI-like concept to clarify value flows, responsibilities, benefits, risk/vulnerability aspects and data needs for evaluation and quality control.	
L4-19	L4	L4 Integration in Logistics	Establish long-term contractual frameworks and risk-sharing models between shippers, logistics operators, OEMs, infrastructure providers and technology providers to support investment in scalable SAE Level 4 freight systems.	New commercial models such as Freight Capacity-as-a-Service, leasing, subscription models, and shared infrastructure investment may reduce adoption barriers. Gap addressed: Current logistics contracts and procurement structures are poorly aligned with the investment profile of autonomous freight systems.

ID	Theme Code	Theme	Recommendation	Motivation (combined)
L4-20	L4	L4 Integration in Logistics	Address trust, perceived controllability, transparency and explainability, and societal acceptance explicitly as deployment requirements for SAE Level 4 freight, treating trust as a dynamic relationship that must be calibrated (avoiding both distrust and overreliance) rather than maximised, and translating these trust-related principles into measurable, verifiable acceptance criteria — including behavioural predictability, public interpretability and perceived operational stability — that complement technical safety evidence in approval and certification.	Societal acceptance and a calibrated, well-founded trust relationship are increasingly central to regulatory approval, certification readiness and long-term deployment legitimacy, and must be made measurable alongside technical safety performance.
L4-21	L4	L4 Integration in Logistics	Ensure conservative, predictable and socially interpretable driving behaviour for heavy automated freight vehicles in mixed traffic — including early signalling, stable lane positioning and conservative gap acceptance — and support it with external HMI and standardised external communication protocols towards surrounding road users, validated through measurable behavioural performance benchmarks and behavioural-consistency assessments across jurisdictions.	Predictable, transparent and socially interpretable behaviour, reinforced by external communication, is a key driver of public confidence and safe interaction in mixed traffic.
L4-22	L4	L4 Integration in Logistics	Maintain a continuously updated ("living") safety case across the full operational lifecycle — covering technical assurance, operational learning, human-factors performance, cybersecurity events and organisational governance, and reflecting over-the-air updates — supported by documented periodic safety reviews, mandatory safety-critical incident reporting, traceable corrective actions and independent audits, so that operational data and human-oversight metrics feed	A living safety case supports ongoing safety assurance, transparency and trust for evolving ADS and links operational learning and human-oversight metrics to approval renewal throughout the lifecycle.

			continuously into risk assessment and approval renewal.	
ID	**Theme Code**	**Theme**	**Recommendation**	**Motivation (combined)**
PI-01	PI	Physical Infrastructure	Establish CCAM-ready infrastructure assessment criteria for corridors, ports, terminals and logistics hubs, covering road geometry, lane markings, signage, maintenance and operational access conditions; connectivity readiness is addressed primarily under digital infrastructure.	This would also enable ports and logistics hubs to position themselves competitively as automation -ready environments The Rotterdam –Oslo corridor analysis showed variability in lane markings, signage consistency, connectivity quality, and digital mapping standards.
PI-02	PI	Physical Infrastructure	Keep road and terminal layouts simple, consistent and machine-interpretable; avoid infrastructure designs that are overly complex or tailored to a single technology provider.	Complex layouts, ambiguous markings, or inconsistent designs increase the likelihood of incorrect interpretation and decision -making. Clear and self -explaining road designs improve comprehensibility for both human drivers and automated driving systems.
PI-03	PI	Physical Infrastructure	Provide safe-haven areas and physical fall-back locations for Minimal Risk Manoeuvres, recovery operations and controlled stops along corridors and inside logistics hubs.	
PI-04	PI	Physical Infrastructure	Define higher maintenance and visibility standards for lane markings, signage and road surface quality to support automated freight operations.	Signs, markings, and pavement need higher maintenance standards to ensure good sensor perception. The required level of maintenance must be developed in collaboration between authorities and the industry.
PI-05	PI	Physical Infrastructure	Deploy infrastructure-based sensing selectively at safety-critical points such as ports, gates, vulnerable road user conflict zones, intersections, loading areas and confined areas.	To ensure legal clarity and functional safety, the vehicle must remain the authoritative decision-making entity. Infrastructure data should therefore be treated as an additional redundancy layer rather than a binding input.

ID	Theme Code	Theme	Recommendation	Motivation (combined)
PI-06	PI	Physical Infrastructure	Enable unmanned physical access to ports, terminals, gates, yards and loading docks, including automated entry, positioning, loading and unloading procedures.	Gap addressed: The current logistics chain is not sufficiently prepared for driverless operations. Business cases remain weak if autonomous vehicles still depend on local personnel for docking, gate access, paperwork, load securing, charging support, or warehouse coordination.
PI-07	PI	Physical Infrastructure	Once harmonised standards are available (e.g. on digital goal posts), implement consistent dock, ramp, loading, unloading and trailer-handling geometry so that automated vehicles can perform precise manoeuvring and logistics operations reliably.	
PI-08	PI	Physical Infrastructure	Prepare charging infrastructure for automated freight vehicles in two steps: first ensure a sufficiently mature heavy-vehicle charging network, then enable physical automation of charging (vehicle positioning, access space, connector handling and scalability for fleets).	
PI-09	PI	Physical Infrastructure	Designate automation-ready zones in industrial areas, ports, terminals and logistics sites to enable early deployment under controlled but scalable conditions.	
PI-10	PI	Physical Infrastructure	Address special infrastructure sections such as tunnels, bridges, tolling points, borders and motorway–urban transitions with dedicated automation-readiness measures.	The German use case addresses the transition from motorway to harbour, including operations in dense traffic and interaction with urban road environments. This scenario exposes challenges related to infrastructure variability, traffic interaction, and system robustness in complex environments.

ID	Theme Code	Theme	Recommendation	Motivation (combined)
PI-11	PI	Physical Infrastructure	Prioritise targeted, scalable and high-impact infrastructure measures, and avoid large-scale physical upgrades where these are not operationally realistic or cost-effective.	The lifetime of road infrastructure is high, and local governments have limited financial resources. Nevertheless, the benefits of infrastructure support are coherent, and CCAM vehicles should use the added value by infrastructure support to improve safety, efficiency and reliability of the automated driving functionality
PI-12	PI	Physical Infrastructure	Aim for alignment between public-road and confined-area infrastructure requirements to avoid operational discontinuities between public roads, ports, yards and terminals.	

ID	Theme Code	Theme	Recommendation	Motivation (combined)
Re-01	Re	Regulation	Allow scalable remote-operator models, including progressive operator-to-vehicle ratios where safety and operational evidence supports them.	Without regulatory acceptance of scalable supervision, AEV business models will not work economically. D1.4 Business models: Current 1:1 supervision models block economic viability.
Re-02	Re	Regulation	Move towards corridor-, route- or service-based approval models that certify the operational system, not only the vehicle.	Permits therefore should be aligned along the logistic chains Therefore, SAE Level 4 vehicles coming from the Netherlands should be able to come to Germany / Hamburg using their SAE Level 4 functionalities.
Re-03	Re	Regulation	Clarify liability and responsibility — distinguishing traffic-safety liability from cargo/goods-related liability — between vehicle manufacturer, ADS provider, infrastructure operator, logistics operator, remote operator and cloud/service providers.	Infrastructure operators cannot assume legal responsibility for perception accuracy due to environmental exposure and varying maintenance conditions. Vehicle manufacturers and operators remain accountable for safety-critical decisions.
Re-04	Re	Regulation	Use performance-based approval criteria that allow approvals to be transferred to comparable operating areas (e.g. extending a campus or road-section approval to similar environments), moving beyond overly static geographical restrictions where sufficient safety evidence is available.	A performance -based, evidence -backed approval model would allow operators to expand geofencing and operational hours based on validated KPIs Gap addressed: Overly conservative operational restrictions currently reduce utilisation and weaken business viability.
Re-05	Re	Regulation	Enable software lifecycle regulation for L4 systems, including updates, validation, monitoring and change management without unnecessary full re-approval.	
Re-06	Re	Regulation	Harmonise cross-border remote-operation rules, including remote-operator licensing, location, supervision responsibilities and intervention authority.	Permits therefore should be aligned along the logistic chains Therefore, SAE Level 4 vehicles coming from the Netherlands should be able to come to Germany / Hamburg using their SAE Level 4 functionalities.

ID	Theme Code	Theme	Recommendation	Motivation (combined)
Re-07	Re	Regulation	Harmonise permit processes across Europe for automated freight trials and deployment — including parallel applications and mutual recognition of safety assessments — so that Member States build on each other's results rather than starting from scratch.	Logistics doesn't stop at national borders. Permits therefore should be aligned along the logistic chains
Re-08	Re	Regulation	(Proposed) Rather than adding new safety-case requirements, align and integrate the SAE Level 4 safety-assurance recommendations with existing regulations (e.g. EU 2022/1426, UNECE R157), clarifying which actor must provide which evidence and how equivalence to a competent human driver is demonstrated.	Regulation currently benchmarks safety to existing human -driven risk levels (e.g., ~10^{-7} fatalities/hour), but public acceptance likely requires significantly higher safety (≈80%+ improvement). D1.2 Safety and security requirements.
Re-09	Re	Regulation	Align deployment with EU Regulation 2022/1426, UNECE Regulation No. 157, ISO 34503, ISO 26262, ISO 21448, ISO 22737, UL 4600 and related regulatory frameworks, and identify potential conflicts with national laws and regulations early.	It is not yet clear how software updates can be handled without redoing a lot of verification and validation work. Automated freight deployment also depends on the interaction between European frameworks and national legal requirements. Potential conflicts should therefore be identified early to avoid barriers during cross-border or corridor-based implementation.
Re-10	Re	Regulation	Clarify legal responsibility for cargo securing, vehicle condition, remote interventions, operational monitoring and incident handling.	Write three to four sentences here
Re-11	Re	Regulation	Ensure GDPR-compliant logging, monitoring and data governance for remote operation, vehicle supervision, infrastructure data and incident investigation.	One of the most significant barriers identified in MODI is uncertainty around accident liability and data access. Insurers and regulators require consistent event logging standards and traceability.

ID	Theme Code	Theme	Recommendation	Motivation (combined)
Re-12	Re	Regulation	Harmonise customs, border-crossing and documentation procedures for automated freight, including digital consignment notes and automated customs interaction.	Addressing these barriers is essential to enable continuous and scalable automated freight operations along European corridors. Remote operation of automated vehicles at border crossings and customs may cause fatalities, injuries and/or damage of other objects.
Re-13	Re	Regulation	Establish clear qualification, training and fitness requirements for remote operators and operational supervisors, including mandatory operator certification, recurrent competency assessments, maximum workload thresholds and minimum communication-redundancy standards, to be demonstrated without unacceptable performance degradation during handovers, degraded-connectivity events and simultaneous alerts.	
Re-14	Re	Regulation	Create regulatory mechanisms for continuous operational monitoring, permit adaptation and permit revocation in case of non-compliance or degraded safety performance.	
Re-15	Re	Regulation	Allow digital-first and risk-based assessment methods, such as digital Site Assessment Tests, remote audits and digital-twin-supported evidence, where they provide sufficient safety assurance for SAE Level 4 CCAM trials and deployments.	

ID	Theme Code	Theme	Recommendation	Motivation (combined)
St-01	St	Standardization	Harmonise safety, ODD, KPI, disengagement, MRM and operational-performance taxonomies across projects, countries and stakeholders.	It would also accelerate permit approvals through transparent performance tracking. MODI partners collected valuable but heterogeneous safety data.
St-02	St	Standardization	Build on the existing V2X and C-ITS message standards (CAM, DENM, MAPEM, SPATEM, CPM, MCM, VAM) and extend or improve them only where gaps exist — e.g. harmonised semantics, quality indicators and confidence levels — rather than re-standardising messages that are already defined.	Common message formats and harmonised use case descriptions helped a lot at the interface between infrastructure and vehicle. Common European standards covering data quality, prediction stability, and confidence indicators are essential to ensure interoperability between infrastructure operators and OEMs.
St-03	St	Standardization	Align vehicle–infrastructure, vehicle–cloud, remote-operation, terminal, gate, charging and logistics interfaces with existing standards (e.g. ETSI), and extend or update them only where concrete gaps for automated freight are identified.	This solves the need for having localization measurement equipment on each vehicle combination. Standardization is necessary to enable large -scale deployment; would enable stakeholders to independently (from ADS supplier or OEM) develop remote operation systems for different types and brands of ADS -equipped vehicles.
St-04	St	Standardization	Standardise logistics and terminal interfaces for gate access, loading, unloading, cargo handover, trailer handling and yard operations.	The Swedish use case focuses on hub -to-hub transport, including automated charging, loading/unloading, and transitions between operational environments. Business cases remain weak if autonomous vehicles still depend on local personnel for docking, gate access, paperwork, load securing, charging support, or warehouse coordination.
St-05	St	Standardization	Standardise automated charging, including physical interfaces, communication protocols, positioning, authentication and operational procedures.	

ID	Theme Code	Theme	Recommendation	Motivation (combined)
St-06	St	Standardization	Aim for interoperability across OEMs, infrastructure providers, map providers, logistics systems and countries before large-scale deployment.	Interoperability testing should therefore be prioritised in future CCAM programmes. As the benefits of C-ITS arise in a multi-domain implementation the roadmaps of implementation should be aligned between infrastructure and vehicles.
St-07	St	Standardization	Develop a common basic road data model with standardised formats for digital maps, routing, and lane-level information to serve as an interoperable foundation across the value chain.	Merging performance was strongly influenced by infrastructure quality, particularly lane markings and map precision. Standardised digital map, routing and lane-level data formats reduce integration effort and support reliable automated manoeuvres. A common basic road data model or profile can further ease exchange between authorities, service providers, map providers and vehicle systems.
St-08	St	Standardization	Harmonise standards for public roads and private/confined logistics areas to avoid incompatible automation environments.	There are separate regulations for private and public areas, e.g. ADS regulation on public road and machine directives on private ground.
St-09	St	Standardization	Avoid proprietary, project-specific solutions and favour open, vendor-independent, modular and updateable standards.	
St-10	St	Standardization	Map, compare and align CCAM deployment with relevant ETSI, ISO, SAE, UNECE, CEN and NAPCORE standards and initiatives, including their scope, location methods, road data models, feature catalogues, APIs and maintenance status.	The CCAM standardisation landscape is broad and fragmented across communication, map, positioning, traffic regulation and data-exchange standards. A structured comparison of standards, their scope, location methods, data models, feature catalogues and maintenance status are needed to identify suitable profiles and avoid inconsistent implementation choices.

ID	Theme Code	Theme	Recommendation	Motivation (combined)
St-11	St	Standardization	Standardise machine-interpretable traffic regulation frameworks, including METR-based approaches, unique identifiers and harmonised feature catalogues for traffic regulations, signs, road markings and signals.	Automated vehicles need consistent digital interpretations of traffic regulations across countries, authorities and service providers. Unique identifiers and harmonised feature catalogues for regulations, signs, road markings and signals reduce ambiguity and support consistent use of machine-interpretable traffic-rule data throughout the value chain.
St-12	St	Standardization	Standardise PKI, certificate management and trust frameworks for C-ITS and V2X communication.	
St-14	St	Standardization	Standardise assessment methodologies, including scenario libraries, pass/fail criteria, sensitivity analyses and impact-assessment indicators.	
St-15	St	Standardization	Use the Enterprise View on the MODI concept (the MODI roles-and-responsibilities model) for MODI-like concept architectures to establish common terminology, shared responsibilities and implementation flexibility across countries and use cases and standardise the relationships between enterprise objects as far as possible to support safety, security, interoperability, scalability and a European 1-to-all interaction model instead of fragmented bilateral arrangements.	[St-15] (no standalone motivation in sources — deliverable/context evidence only) [St-22] (no standalone motivation in sources — deliverable/context evidence only)
St-16	St	Standardization	Establish a common agreement framework for enterprise objects involved in MODI-like SAE Level 4 CCAM operations and standardise agreements as far as possible or base them on common templates to support equal treatment and consistent service quality across European actors.	

ID	Theme Code	Theme	Recommendation	Motivation (combined)
St-17	St	Standardization	Standardise the interface by which an automated vehicle, or an authorised entity acting on its behalf, requests authorisation to enter an infrastructure authority domain and provides monitoring-relevant vehicle data independent of make and model.	
St-18	St	Standardization	Develop European profile standards for GNSS augmentation/enhancement and non-GNSS local positioning systems used by automated vehicles, including communication profiles, accuracy/availability requirements and fusion of positioning data sources.	Measures to improve GNSS quality are important to gain the positive effects of C-ITS Services This could be seen in all three C-ITS services in the UC Germany.
St-19	St	Standardization	Standardise the generation and exchange of heavy-vehicle drivable corridors by specifying how routing maps, perception data, drivable-space representations, and V2X inputs are integrated into actionable corridor definitions.	
St-20	St	Standardization	Define standardised accuracy, uncertainty and confidence requirements for sensor-derived data elements embedded in V2X message containers, especially where cooperative data may support safety-relevant functions.	A common classification is necessary for the success of cooperative perception systems by testing and evaluating the VRU service within the use case Germany it became apparent, that the object classification is different between the vehicle and the infrastructure.
St-21	St	Standardization	Define congestion-control requirements and adaptive communication strategies for dense V2X environments to ensure reliable delivery of critical messages under high communication load.	

ID	Theme Code	Theme	Recommendation	Motivation (combined)
St-23	St	Standardization	Develop a European profile standard for the applications and services exchanged between roadside (ITS Field) systems and in-vehicle (ITS Vehicle) systems, covering traffic-regulation execution, infrastructure and environmental data, and ITS services relevant to automated driving.	To foster the roll out of cooperative infrastructure, C-ITS equipment should be part of the construction standard of traffic. Efficient autonomous freight operations require continuous real-time data exchange across organisational boundaries.
St-24	St	Standardization	Standardise secure and interoperable interfaces for remote operation between remote-operator personal devices or central remote-operation systems and ITS Vehicle systems, including cargo sensor interfaces where remote operators need cargo status for assistance, incident handling or monitoring.	A CEN API will enable an interoperable, secure, flexible, and effective Remote Operation covering both Remote Assistance and Remote Driving of automated vehicles moving around in European border areas, customs areas, harbours, terminals, and physical infrastructure for road vehicles. Lack of such an API is expected to cause the development of proprietary solutions that will be a major challenge and obstacle for operators of automated vehicles and operators of borders, customs, other confined areas and public roads.
St-25	St	Standardization	Standardise the interface between infrastructure traffic management systems and ITS Vehicle systems to enable secure, interoperable and cross-border traffic management of automated vehicles within physical-infrastructure authority domains.	However, there is no scalable framework in which private confined area operators can take up this digital traffic management capability by building/licencing private traffic management platforms and integrate with public traffic management systems in the vicinity. MODI has taught us that SAE Level 4 vehicles need local and real -time traffic management context both on public and private road, to drive safely and efficiently.

ID	Theme Code	Theme	Recommendation	Motivation (combined)
St-26	St	Standardization	Standardise CEN/ISO C-ITS-based APIs between vehicle on-board equipment and authorised roadside or personal equipment in border, customs and enforcement contexts to enable secure access to vehicle/cargo information, routing instructions and emergency or control services.	A CEN API will enable border and customs officers and other authorized persons, e.g., police and road authorities, to access the information about the vehicle and possibly the goods being transported, at borders and customs. The interface should also include services and data that enables border and customs officers to stop the automated vehicle in emergency situations.

Annex II: Enterprise View on MODI Concept

Introduction

This document describes a proposal for an Enterprise View on the MODI concept. The Enterprise View is based on the ARC-IT architecture used in ISO TC 204 ITS architecture documents. More information on the four architecture views Enterprise View, Physical view, Functional view, and Communication view is available on https://www.arc-it.net/.

The Enterprise View consists of enterprise objects, aka roles and stakeholders, and their relationships to other enterprise objects. As such, it is an extension of a role and responsibility model. There are two types of relationships in the model: a contractual relationship and an expectation relationship. The expectation relation describes the information and services one enterprise object expects from another enterprise object. The model may also include how an enterprise object interacts, e.g., owns, operates, develops, installs, maintains, etc., with physical objects called Resources in the model.

The model in this document describes a generic view on contractual relationships. The contractual relationships may differ from one region, country or use case.

Enterprise View

Introduction

Figure 1 shows the complete Enterprise View of the MODI concept. The enterprise objects, which can be persons, organisations, companies, authorities, and any other types of stakeholders, are shown as light green boxes. The relationships between the enterprise objects are the main expectations shown as blue dashed arrows. The only physical object shown is the Automated vehicle.

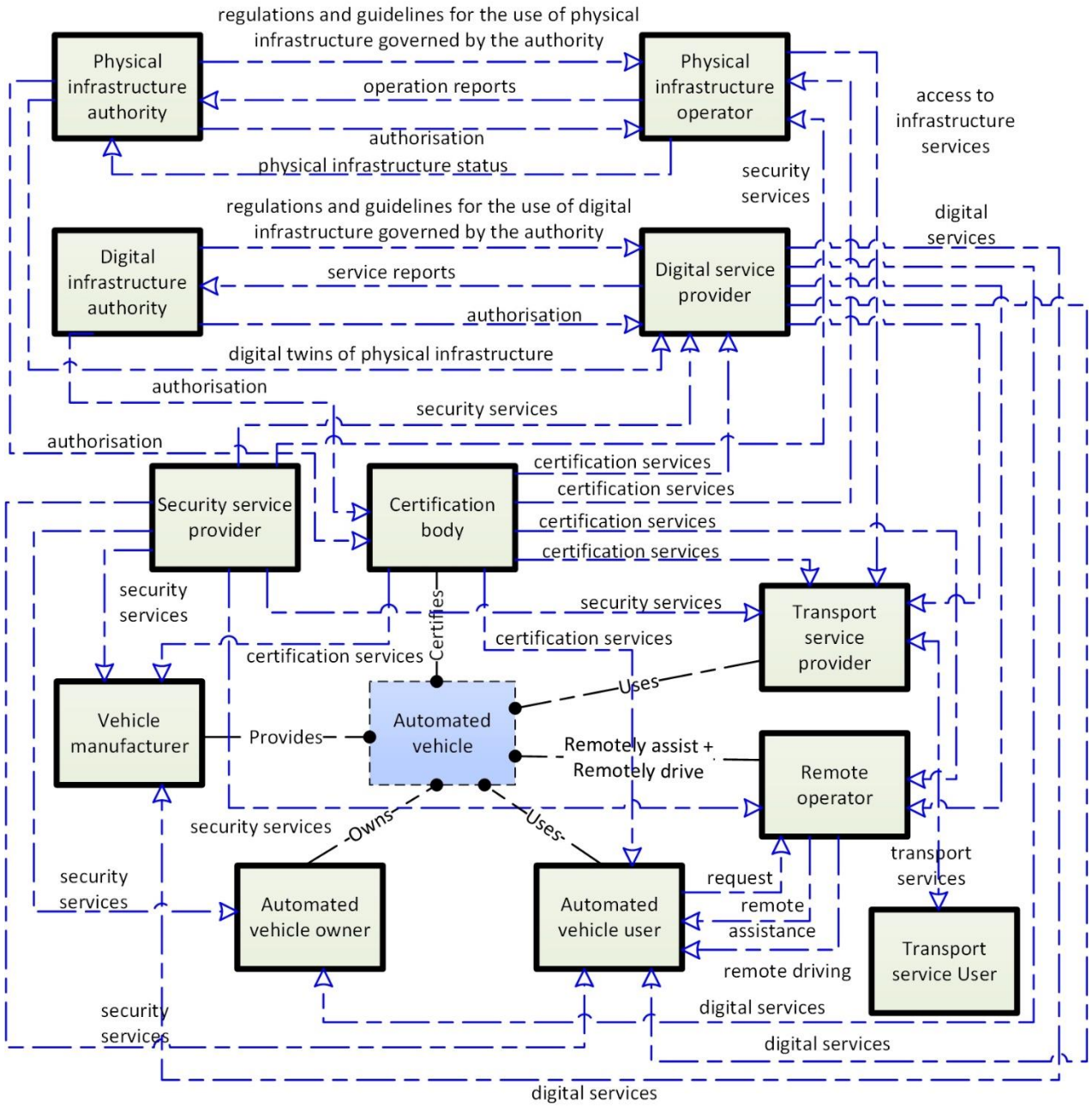


Figure 1: The complete Enterprise View of the MODI concept

Enterprise objects and their expectations

The enterprise objects in Figure 1 are described in the following subclauses in alphabetic order.

Automated vehicle owner

The Enterprise object Automated Vehicle Owner owns the automated vehicle. The Automated vehicle owner could also be the Automated vehicle user and vice versa.

The Automated vehicle owner has the following responsibilities:

- Register the automated vehicle as defined in the regional and national registration regulations
- Maintain the automated vehicle as defined in the regional, national, and local rules and regulations for the use and maintenance of automated vehicles
- Pay the required fees, tolls, taxes, insurances, maintenance costs etc. related to the use of the automated vehicle on public roads and confined areas
- Monitor the use of the automated vehicle
- Ensure that the vehicle fulfils the security and safety requirements for the automated vehicle by certification by an authorised provider of certification services
- Ensure that any other transport service user using the automated vehicle for transport services is certified for the use
- Ensure that any transport service provider using the automated vehicle for delivering transport services, e.g., moving persons or goods, is certified as a service provider for the actual transport service
- Ensure that any provider of remote assistance and/or remote driving services that gets access to the automated vehicle, is certified for delivering these types of services
- Comply with the security architecture requirements for access to the automated vehicle, e.g., for monitoring and collection of maintenance and usage data
- Enter an agreement with the Automatic vehicle user in cases where the user is not the same legal entity as the owner

The Automatic vehicle owner has the following expectations from other enterprise objects:

- Security services from the Security service provider enabling the owner to access the Vehicle ITS system, aka On-Board Equipment (OBE), in a secure way
- Digital services from the Digital service provider enabling the owner to communicate with the Vehicle ITS system for exchange of information

Examples on legal entities being Automatic vehicle owners are a natural person or a legal entity, including companies, public authorities, and non-profit organizations, provided that the owner can be uniquely identified and held legally and financially responsible.

Automated vehicle user

The Enterprise object Automated vehicle user uses the automated vehicle for his/her own purposes or for providing transport services like transport of persons and goods. The Automated vehicle user could also be the Automated vehicle owner and vice versa.

The automated vehicle user has the following responsibilities:

- operate the automated vehicle as defined in the regional, national, and local rules and regulations for the use of automated vehicles
- monitor the use of the automated vehicle
- have the required certification to operate the automated vehicle
- comply with the security architecture requirements for access to the automated vehicle,
- request remote assistance whenever the Vehicle ITS system does not request remote assistance in situations where the Vehicle ITS system including the Automated Driving System is not able to handle the situation and the situation can be solved by remote assistance

- request remote driving whenever the remote assistance is not solving the situation that required remote assistance
- enter an agreement with the Automatic vehicle owner in cases where the user is not the same legal entity as the owner

The Automatic vehicle user has the following expectations from other enterprise objects:

- security services from the Security service provider enabling the user to access the Vehicle ITS system, aka On-Board Equipment (OBE)
- digital services from the Digital service provider enabling the user to operate the automated vehicle
- remote assistance from the Remote operator in incidents where the Vehicle ITS system including the Automated Driving System (ADS) cannot handle the incident preventing the automated vehicle to continue its mission
- remote driving from the Remote operator in incidents where the remote assistance did not solve the problem(s) related to the incident and where a certified remote driver can solve the problem enabling the vehicle to continue its mission or perform a Minimum Risk Manoeuvre

Examples on legal entities being Automatic vehicle users are a natural person or a legal entity, including companies, public authorities, and non-profit organizations, provided that the user has an owner-user agreement with the Automated Vehicle Owner in those cases where the owner and user is not the same legal entity.

Certification body

The certification body is an entity that is authorised by a physical and/or a digital authority, or any other relevant authority, to certify the MODI relevant Enterprise, Physical and Functional objects.

The certification body has the following responsibilities:

- certify Physical infrastructure operators ensuring that their organisation and operation of the physical infrastructure is fulfilling the requirements for automated driving and that the physical infrastructure, including Roadside ITS systems, is compliant with the claimed Operational Design Domain (ODD)
- certify Digital service providers ensuring that their organisation and operation of the digital infrastructure is fulfilling the requirements for automated driving on the relevant SAE and security level and that the digital infrastructure installed and operated in the physical infrastructure is compliant with the claimed Operational Design Domain (ODD)
- certify Transport service providers ensuring that their provision of transport services based on automated vehicles fulfils the safety and security requirements needed for automated transport of persons and goods on public roads and confined areas. The term transport services also cover services related to transport, e.g., charging of electric vehicles, automated loading/unloading, border crossings including customs.
- certify Remote operators, i.e. entities that provide remote assistance and/or remote driving services ensuring that the remote assistants and the remote drivers have the required level of competence, e.g., knowledge and experience, to provide remote assistant and driving services. The certification could be limited, e.g. to specific geographic areas and specific types of vehicles.

- certify Automated vehicle users ensuring that the users have the required level of competence, e.g., knowledge and experience, to operate the automated vehicle. The certification could be limited, e.g. to specific geographic areas (public roads and confined areas) and specific types of vehicles.
- certify Vehicle manufacturers ensuring that their development, testing, production, and quality assurance systems fulfil the regional and national requirements for manufacturing of automated vehicles
- certify automated vehicles ensuring compliance with regional and national requirements for automated vehicles

The Certification body has the following expectations from other enterprise objects:

- authorisation by a Physical infrastructure authority to certify relevant enterprise, physical and functional objects
- authorisation by a Digital infrastructure authority to certify relevant enterprise, physical and functional objects

Digital infrastructure authority

The digital infrastructure authority is a legal entity that develops, manages and publish laws, regulations and guidelines for the use of digital infrastructure governed by the authority, e.g. infrastructure used for communication and positioning services related to automated vehicles. The Digital infrastructure authority has the following responsibilities:

- develop, manage, and publish laws, regulations and recommendations for the use of digital infrastructure governed by the authority
- manage service and operational reports from the providers of digital services, and use the reports for monitoring and improving the provision of the digital services
- authorise Digital service providers to provide digital services to automated vehicles and other Enterprise objects after the Digital service providers have been certified by an authorised certification body
- solve any conflict between the Digital service providers and the users of these services

The Digital infrastructure authority has the following expectation from other Enterprise objects:

- service reports from the Digital service provider, enabling the Digital service authority to monitor the provision of digital services and improve the specifications for the services

Examples on Digital infrastructure authorities are Communication authorities, Data Protection Authority, Map authorities, Positioning systems authorities, electronic traffic rules and regulation authorities and Road authorities that e.g., manages national road data bases.

Digital service provider

The Digital Service provider is an entity that supports other Enterprise objects with digital services needed for their fulfilment of responsibilities. The Digital service provider has the following responsibilities:

- implement the laws, regulations and recommendations from the different Digital infrastructure authorities and prove by certification that they are implemented

- request authorisation from the Digital infrastructure authority to operate as a digital service provider within the jurisdiction of the Digital infrastructure authority. The request is for simplicity reasons not shown in Figure 1.
- implement the security services provided by the Security service provider and prove by certification that they are implemented.
- use the certification services provided by authorised Certification bodies and forward the certification to the Digital infrastructure authority as part of the authorisation request
- receive, manage, and distribute digital twins of the physical infrastructure governed by Physical infrastructure authorities, e.g., road authorities and confined area authorities.
- report on digital services provided enabling the Digital infrastructure authority to monitor the services provided

The Digital service provider has the following expectations from other Enterprise objects:

- regulations and guidelines for the use of digital infrastructure from the Digital infrastructure authority
- authorisation from the Digital infrastructure authority to provide digital services enabling the use and operation of automated vehicles
- digital twins of physical infrastructure that are continuously updated from the Physical infrastructure authority for further management and distribution by the Digital service provider to the automated vehicle, e.g. as HD maps and electronic traffic regulations
- Certification services from the authorised Certification body

Physical infrastructure authority

The Physical infrastructure authority is a legal entity that develops, manages and publish regulations and guidelines for the use of physical infrastructure governed by the authority, e.g. infrastructure used for transport of goods and persons on roads and infrastructure for vehicles in confined areas, e.g., terminals and harbours. The Physical infrastructure authority has the following responsibilities:

- develop, manage, and publish regulations and guidelines for the use of physical infrastructure governed by the authority
- manage operational reports from the operators of physical infrastructure for automated vehicles and use the reports for monitoring and improving the physical infrastructure
- authorise Physical infrastructure operators to operate physical infrastructure after the physical infrastructure operators have been certified by an authorised certification body
- solve any conflict between the physical infrastructure operator and the users of the infrastructure.

The Physical infrastructure authority has the following expectation from other Enterprise objects:

- Operation reports from the Physical infrastructure operator, enabling the Physical infrastructure authority to monitor the operation of the physical infrastructure, e.g., traffic management, maintenance, safety, critical incidents and the implementation of regulations and guidelines.
- Physical infrastructure status enabling the Physical infrastructure authority to continuously update the digital twin of the physical infrastructure governed by the Physical Infrastructure authority and used for automated driving.

Examples on Physical infrastructure authorities are Department for Transport, Public roads authorities and Confined areas authorities like Harbour authorities.

Physical infrastructure operator

A Physical infrastructure operator is an entity that operates physical infrastructure used by automated vehicles. The main responsibilities of the physical infrastructure operator are:

- Implement the regulations and guidelines from the different physical infrastructure authorities and prove by certification that they are implemented
- Build, operate and maintain the physical infrastructure enabling the use of automated vehicles for transport of goods and persons in line with regulations and guidelines
- Request authorisation from the Physical infrastructure authority to operate the physical infrastructure within the jurisdiction of the physical infrastructure authority. The request is for simplicity reasons not shown in Figure 1.
- Implement the security services provided by the Security service provider and prove by certification that they are implemented. This is relevant both for any central system and for any roadside system needed for the operation of the physical infrastructure.
- Use the certification services provided by authorised Certification bodies and forward the certification to the Physical infrastructure authority as part of the authorisation request
- Continuously collect data on the status of the physical infrastructure and forward the data to the Physical infrastructure authority enabling a continuously update of the digital twin of the physical infrastructure for automated driving.
- Report to the Physical infrastructure authority on the operation of the physical infrastructure enabling the Physical infrastructure authority to monitor the operation of the infrastructure it governs.

The Physical infrastructure operator has the following expectation from other Enterprise objects:

- Regulations and guidelines for the use of physical infrastructure from the Physical infrastructure authority
- Authorisation from the Physical infrastructure authority to operate a physical infrastructure governed by the Physical infrastructure authority enabling the use and operation of automated vehicles
- Certification services from the authorised Certification body
- Security services from the Security service provider

Examples on physical infrastructures operators are operators of confined areas, e.g. ports, consolidation centres, terminals, and public road operators and contractors for road operation.

Remote operator

A Remote operator covers two sub-enterprise objects: the Remote assistant and the Remote driver. The Remote assistant aids the user of the automated vehicle when there is a situation where the Vehicle ITS system including the Automated Driving System cannot carry through the mission of the automated vehicle. The Remote driver provides remote driving services in those cases where the situation/incident cannot be solved by remote assistance.

The Remote assistant has the following responsibilities:

- Request certification from an authorised Certification body after having implemented the Physical and Digital infrastructure authority requirements for remote assistance. The request and the Physical and Digital infrastructure authority requirements for remote assistance are for simplicity reasons not shown in Figure 1.
- Implement the security services provided by the Security service provider and prove by certification that they are implemented.
- Provide remote assistance to Automated vehicle users that have requested such services, either from the Automatic vehicle user (human user) or from the Vehicle ITS system including the Automated Driving system
- Use the digital services provided by the Digital service provider for the remote assistance

The Remote driver has the following responsibilities:

- Request certification from an authorised Certification body after having implemented the Physical and Digital infrastructure authority requirements for remote driving. The request and the Physical and Digital infrastructure authority requirements for remote driving are for simplicity reasons not shown in Figure 1.
- Implement the security services provided by the Security service provider and prove by certification that they are implemented.
- Provide remote driving to Automated vehicle users that have requested such services, either from the Automated vehicle users (human user or) from the Vehicle ITS system including the Automated Driving system
- Use the digital services provided by the Digital service provider for the remote driving

The Remote operator has the following expectation from other Enterprise objects:

- Security services from the Security service provider
- Digital services from the Digital service provider
- Certification services from Certification body
- Request from the Automated vehicle user or from the Vehicle ITS system including the Automated Driving system (the last alternative is not shown in the Figure 1)

Examples on Remote operators can be vehicle manufacturers that can support their own makes and models or Trusted Third Parties (TTP) that have the required digital infrastructure and trained and certified personnel to handle any vehicle make and model. The last alternative requires a European standardised interface for remote operation ensuring safety, security and interoperability on a European level.

Security service provider

A Security service provider is an entity that supports most of the Enterprise objects in Figure 1 with security services providing as a minimum the security measures confidentiality, integrity and availability. The Security service provider has the following responsibilities:

- Develop, maintain, and operate a security scheme based on European legislation, directives and regulations and European and international security standards ensuring the required level of security, safety, interoperability and confidence in automated driving.
- Support all Enterprise objects and their Physical and Functional objects with security services ensuring a high level of cyber security meaning the practice of protecting systems, networks, programs, and data from digital attacks, unauthorized access, and damage.

- Monitor the implementation by the Enterprise objects of the required security measures and mechanisms
- Manage any security incident detected or reported by an Enterprise object or the Physical objects owned, operated, or used by the Enterprise object

It is of major importance that the Vehicle manufacturers become Enterprise objects that are part of the security architecture. The communication with the automated vehicle is over-the-air which is a vulnerable interface with standardised messages that can be listened to, copied, replayed, or changed. Mutual authentication and the use of Public key infrastructure (PKI) mechanisms will support confidentiality and integrity.

Transport service provider

A Transport service provider is an entity that provides a transport service to the Transport service user. Examples on transport services in the MODI context are access to public roads, transport of goods, access to confined areas, loading/unloading of goods, customs handling, border crossings and charging of electric vehicles.

The Transport service provider has the following responsibilities:

- Provide Transport services to Transport service users based on their requirements and preferences for the transport service and the use of automated vehicles (shown as a two-way expectation in Figure 1)
- Get access to physical infrastructure needed for the provision of the transport service, e.g., access to public roads and confined areas
- Implement the required digital services that are offered by the digital service providers as part of the MODI concept and required for fulfilling the Transport service provider responsibilities
- Adhere to the security framework to the extend required for the provision of the transport service and the transport service user security and confidence in transport services using automated vehicles.
- If required, be certified by a relevant certification body as a user of automated vehicles for the provision of transport services

The Transport service provider has the following expectations:

- Access to infrastructure services from the Physical infrastructure operator
- Digital services from the Digital service provider
- Security services from the Security service provider
- Request for transport services (included in the two-way expectation between Transport service provider and Transport service user)
- Certification services from the Certification body

The Transport service provider and the Automated vehicle user can be the same legal entity ensuring that the Transport service provider has access to important information provided by the automated vehicle as well as e.g., rerouting the automated vehicle caused by incidents like closed roads, queues, traffic accidents, bad weather, delays at a terminal, etc. If they are not the same legal entity there is a need for an agreement between the two enterprise objects ensuring the same functionality and security as if they were the same legal entity. These relations are for simplicity reasons not shown in Figure 1.

Examples on Transport service providers are carriers, road and confined area operators, customs and terminal operators and charging stations operators.

Transport service user

The Transport service user is an entity that requests and uses transport services provided by a Transport service provider. The Transport service user has the following responsibilities:

- Request a transport service from a Transport service provider based on the user needs and preferences
- Accept an offer from the Transport service provider and accept that the transport service will include the use of automated vehicles
- Use the transport service and if required, pay for the service

The Transport service user has the following expectations:

- An offer from the Transport service provider based on the service user request
- A transport service based on the accepted offer

The bilateral expectations between the Transport service user and the Transport service provider are covered by the two-way expectation called transport services in Figure 1.

Vehicle manufacturer

The Vehicle manufacturer is an entity that designs, develops, tests, produces, and sells automated vehicles to Automated vehicle owners. The Vehicle manufacturer has the following responsibilities:

- Design, develop, test and produce automated vehicles fulfilling the quality, safety and security requirements defined in European legislation, directives, and regulations, UNECE regulations and requirements and European and international vehicle standards guaranteeing the required level of security, safety, and confidence in automated vehicles.
- Have the automated vehicle certified for automated driving by an authorised Certification body
- Implement the required security measures and mechanisms that as a minimum ensures confidentiality, integrity, and availability and where the measures and mechanisms are based on security requirements defined in European legislation, directives and regulations, and European and international security standards
- Implement the standardised digital services enabling European interoperability between the automated vehicle and the enterprise objects that exchange information and services with the automated vehicle.

The Vehicle manufacturer has the following expectations:

- Security services from Security service provider
- Certification services from Certification body
- Digital services from Digital service providers

Enterprise objects and their agreements

The relationships between the Enterprise objects should be organised by an agreement framework ensuring an unambiguous and collective understanding of responsibilities and prerequisites for the

partners entering an agreement. Figure 2 shows the proposed agreement framework for the MODI concept. The different types of agreements are listed below the figure.

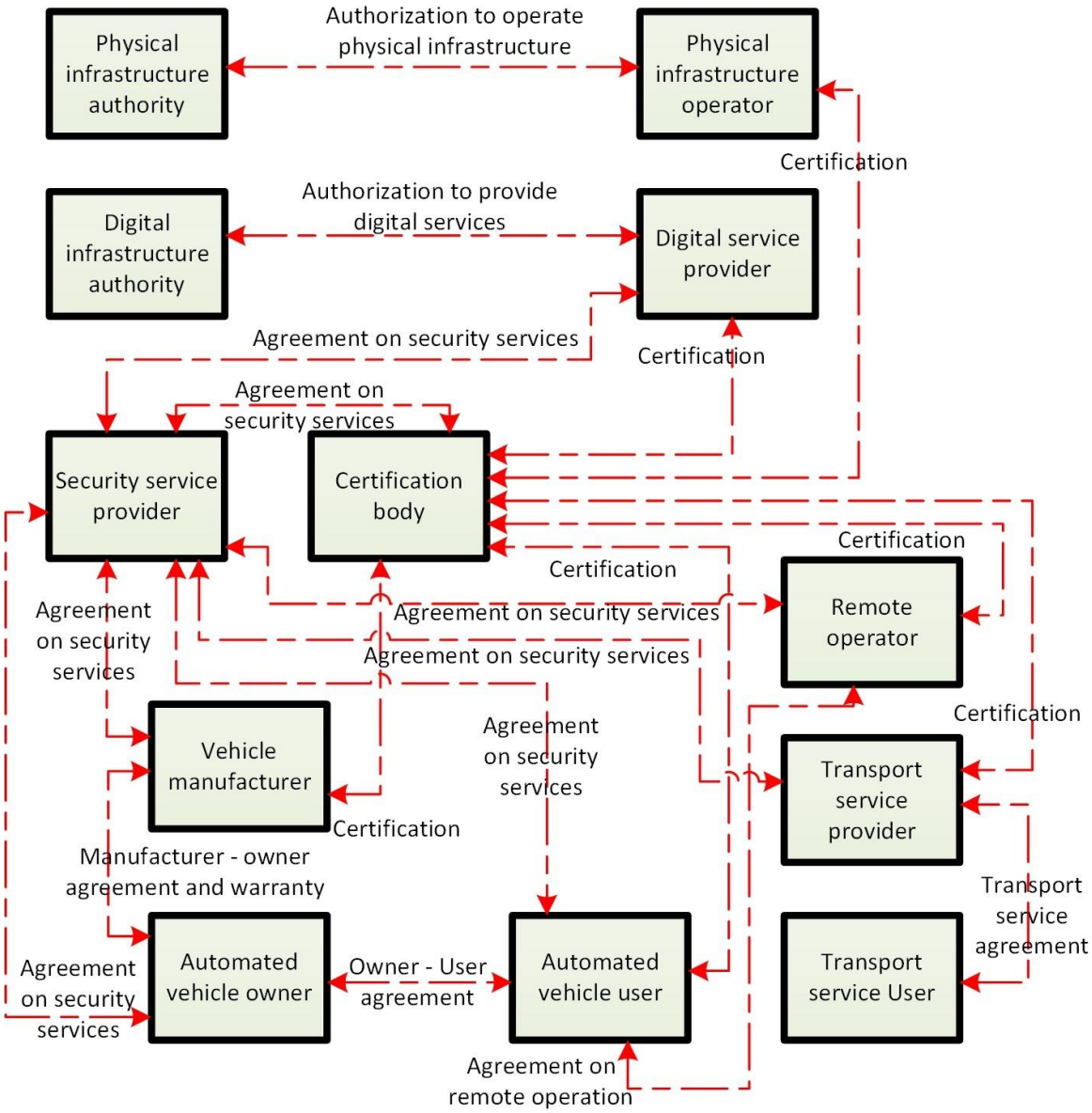


Figure 2: Agreement framework for the MODI concept

The following types of agreements are listed below.

- **Authorization to operate physical infrastructure** covers the agreement between a Physical infrastructure authority and a Physical infrastructure operator. The agreement can be implicit, e.g., a legal framework, e.g., laws and regulations, describes the responsibilities and prerequisites for the operation of certain physical infrastructure, e.g. public roads. The agreement can also be explicit, e.g. a harbour authority enters an agreement with a contractor to operate the physical infrastructure in a harbour.
- **Authorisation to provide digital services** covers the agreement between a Digital infrastructure authority and Digital service provider. A telecommunication authority can for

instance enter into agreements with owners and operators of cellular networks used for communication between Enterprise objects or operators supporting intelligent transport system services. An operator of a local positioning system used in a confined area may request a national communication authority to be authorised to use a bandwidth governed by the national communication authority. A road operator may in the same way request the authorisation for the use of Roadside equipment (RSE) transmitting information to automated vehicles within a bandwidth governed by the national communication authority.

- **Agreement on security services** covers the agreement between the Security service provider, e.g. a Trusted Third Party, and the enterprise objects that must adhere to the security policy of the MODI concept which again will be based on European directives and security and certificate policies. The content of the agreement will depend on the responsibilities of the enterprise objects and the security threats related to the different enterprise objects. E.g., the agreement between the Security service provider and a Vehicle manufacturer will be quite different from the agreement between the Security service provider and the Automated vehicle owner that may only require access to specific data collected by the automated vehicle.
- **Certification** covers the agreement between a Certification body and an enterprise object that should be certified ensuring the safety and security related to automated driving. There will be different certification bodies for different enterprise objects, e.g. certification bodies that can certify Digital service providers and certification bodies that can certify Remote operator personnel.
- **Agreement on remote operation** covers agreements between the Automated vehicle user and the providers of remote assistance and remote driving services. It is foreseen that providers of remote assistance service and providers of remote driving services may be the same legal entity, but they may also be different legal entities due to different responsibilities and different requirements for the personnel involved in the provision of the services.
- **Transport service agreement** covers the agreement between the Transport service provider and the Transport service user. As there will be a range of different transport services, there will be a range of different agreements. However, the involvement of an automated vehicle in the transport service will be common for all agreements.
- **Owner – User agreement** covers the agreement between the Automated vehicle owner and the Automated vehicle user in cases where the two enterprise objects are not the same legal entity. There is an important need for an unambiguous agreement and a collective understanding of the responsibilities of the two parties, e.g., when unwanted or unexpected incidents occur.

Recommendations

Table 1: Recommendations "Enterprise View"

Recommendation for the Enterprise View on the MODI concept (aka MODI roles and responsibilities model)	
Rec D1.5- 1.	**Recommendation**: The Enterprise View on the MODI concept (aka MODI roles and responsibility model) should be used for concept architectures like the MODI concept
	Motivation: It is crucial that the involved stakeholders in concepts like MODI should have a common understanding of the concept based on a common enterprise model ensuring common terminology and a common allocation of responsibilities to the enterprise objects in the model. The abstract enterprise objects enable full flexibility concerning the different actors that can fulfil the different responsibilities for each abstract enterprise object and allows for national and local implementations of the MODI concept.
Recommendation for the relationships between the enterprises in the MODI concept	
Rec D1.5- 2.	**Recommendation**: The relationships between the enterprise objects in the Enterprise View model should as far as possible be standardised ensuring safety, security and interoperability on a European level for concepts like MODI
	Motivation: Standardisation supports interoperability, scalability and widespread deployment, safety and reliability, data consistency and quality, and value networks models. There will be many enterprise objects on a European level and a 1:1 relationship between all the enterprise objects seems unrealistic. A concept where there is a 1:all relationship seems the only way forward in achieving effective, safe, secure and reliable MODI-like concepts on a European level.
Recommendation for the agreements between the enterprise objects	
Rec D1.5- 3.	**Recommendation**: There should be common agreement framework for all enterprise objects in MODI-like concepts and the agreements in the framework should as far as possible be standardised, or as a minimum be based on common templates supporting equality between all European actors that will fulfil all or parts of the different enterprise responsibilities.
	Motivation: The main motivation behind the recommendation is to ensure equality between all possible European actors that could fulfil parts of or all responsibilities of one or more enterprise object responsibilities. Another motivation is that a common agreement framework will ensure a common level of quality for services and information exchanged between the enterprise objects.

Annex III: Trust, Human Factors and Public Acceptance in Level 4 Automated Freight Transport

Introduction

Technical capability alone is insufficient for the large-scale deployment of SAE Level 4 automated freight transport. Experience from lower SAE automation levels, remote operations, aviation, and broader human-automation research demonstrates that societal acceptance depends heavily on:

- Trust
- Predictability
- Transparency
- Perceived controllability

These dimensions are not only operational concerns but are increasingly central to regulatory approval, certification readiness, and long-term deployment legitimacy. As SAE Level 4 systems move toward commercial operation, regulators and certification authorities will require evidence that human factors, organizational governance, and public interaction risks are addressed systematically alongside technical safety performance [1,2,3]

Within MODI, trust should not be viewed as a simple binary state in which stakeholders either trust the system or do not. Rather, trust emerges as a dynamic and continuously evolving relationship between people, automated systems, organizations, infrastructure and the broader operational environment. It develops through ongoing interactions, observed system behaviour, organizational performance and operational experience, and is influenced by how effectively these interconnected elements work together under both normal and degraded conditions

Trust evolves through repeated operational experience, observed system behaviour, the quality of communication, and the demonstrated ability of a system to operate safely under both routine and degraded conditions [1,2,3,6]. As confidence in automated systems is built gradually over time, governance and certification frameworks must move beyond purely technical performance metrics and incorporate mechanisms that ensure transparency, operator competence, effective incident reporting, robust fall-back performance, meaningful human oversight, and continuous operational monitoring. By translating these trust-related principles into measurable and verifiable requirements, regulators and certification authorities can provide assurance that automated systems remain safe, understandable, accountable and worthy of public confidence throughout their operational lifecycle [4,17,19,20].

Factors influencing trust, public acceptance, and regulatory readiness.

MODI activities highlighted several factors influencing trust, public acceptance, and regulatory readiness.

1. Technical safety and societal trust may evolve differently

Technical safety performance and societal trust do not necessarily mature at the same pace. Even rare failures may disproportionately influence public perception and confidence [5,7,8,9].

For example, simulated emergency braking events during demonstration activities showed that, even when the automated system responded correctly, nearby observers often interpreted abrupt manoeuvres as signs of instability. Regulatory and certification processes should therefore consider not only collision avoidance performance in standardized test procedure with dummy road users but also:

- Behavioural predictability
- Public interpretability
- Perceived operational stability [1,2,3,6].

These elements should form part of operational acceptance criteria [12,13,14].

2. Trust Must Be Properly Calibrated

Trust should be calibrated rather than maximized. Both distrust and overreliance can create operational safety risks [1,2,3,10].

During remote supervision exercises, operators may become overly confident in stable motorway performance and react more slowly when unexpected roadworks or lane closures appear [1,2,3,6].

Note! Although the ego SAE Level 4 vehicle ideally should know when a road event is outside the vehicle ODD there are cases where the vehicle or geofencing is insufficient. Certification frameworks should therefore include requirements for:

- Human oversight capability
- Operator engagement monitoring
- Workload management
- Clear allocation of responsibility between automation and remote personnel [6,12].

3. Predictable and Understandable Vehicle Behaviour Is Essential

Predictable, conservative, and socially understandable vehicle behaviour is particularly important for heavy automated freight vehicles operating in mixed traffic [5, 8,12.13,14].

Surrounding drivers react more positively when automated trucks demonstrate

- Early signalling
- Smooth lane positioning
- Conservative gap acceptance at merges and intersections

External HMI and transparent operational communication [3,6,14,20]. may further support public confidence. Governance frameworks should translate these findings into:

- Operational design domain expectations

- Behavioural performance benchmarks
- Harmonized guidance for interaction with other road users

4. Remote operations depend on a broader trust ecosystem

Remote operations form part of a distributed socio-technical trust ecosystem [6,12,13,20]. involving:

- Operators
- Communication infrastructure
- Organizations
- Automation systems

As a result, situation awareness, workload management, alarm prioritization, and controllability become central design considerations.

Exercises involving remote operator handover during temporary connectivity degradation demonstrates how delayed video feeds and competing alarms could reduce operator confidence and increase cognitive workload [14,15]. Regulatory oversight should therefore extend beyond the vehicle itself to include:

- Remote operation centres
- Communication resilience
- Staffing models
- Training obligations
- Organizational safety management systems

5. Degraded-mode behaviour strongly influences public trust

Public trust is strongly influenced by how systems behave during:

- Degraded modes
- Fall-back situations
- Connectivity loss
- Cyber incidents
- Emergency handling [17,19,20].

Closed-course testing involving controlled GNSS degradation and communication dropouts demonstrates the importance of safe fall-back strategies such as minimal risk stops and clear operator notification procedures.

Certification authorities should therefore require demonstrable evidence that:

- Degraded-mode handling is validated
- Cybersecurity resilience is tested
- Emergency response coordination functions effectively under realistic operational conditions

6. Human-centred automation extends beyond engineering performance

Human-centred automation requires systems to be designed not only around engineering performance but also around:

- Human perception

- Cognition
- Organizational behaviour
- Social interaction [16,24].

MODI safety testing and validation with experts and stakeholders indicate that understandable operational procedures and clear escalation responsibilities during abnormal events can be important for logistics personnel and emergency responders, customs etc. [12,13,14].

Governance frameworks should therefore embed:

- Human factors engineering
- Stakeholder communication
- Organizational accountability

For example, does the SAE Level 4 vehicle allow customs or police to contact and speak to remote operators by a speech acoustic interface on the vehicle. These elements should be integrated directly into approval and compliance processes rather than treated as secondary considerations [20].

Strategic recommendations

MODI highlights four strategic priorities related to trust, societal acceptance, and regulatory implementation. Each priority should be translated into enforceable certification and compliance obligations supported by measurable assessment criteria.

1. Establish and maintain a living safety case

Operators and manufacturers should maintain a continuously updated living safety case [17,19,20]. covering:

- Technical assurance
- Operational learning
- Human factors performance
- Cybersecurity events
- Organizational governance

This safety case should remain active throughout the operational lifecycle. **Note!** SAE Level 4 vehicles will be under continuous change/improvements by over the air updates

Compliance Requirements

Compliance should include:

- Documented quarterly safety reviews
- Mandatory reporting of all safety-critical incidents within defined regulatory timelines
- Traceable corrective action processes
- Annual independent audits of safety governance procedures

Certification authorities should verify that operational data, incident trends, and human oversight metrics are incorporated into ongoing risk assessments and approval renewals.

Suggested KPIs

- Incident reporting closure rate
- Percentage of corrective actions implemented within required deadlines
- Frequency of safety case updates
- Operator intervention rates
- Audit non-conformance resolution time

2. Require structured validation before public-road deployment

All SAE Level 4 freight systems should complete structured closed-course sandbox, and/or simulation, and validation programmes prior to public-road deployment [4,12,13,].

Testing should include:

- Degraded modes
- Remote operations
- Connectivity loss
- Emergency fall-back behaviour
- Edge-case scenarios representative of the intended operational design domain

Compliance Requirements

Compliance should require documented evidence that predefined performance thresholds are achieved under repeatable test conditions and independently validated by competent authorities or accredited third parties.

Certification assessments should evaluate both:

- Technical safety outcomes
- Human-system interaction performance indicators

Examples include operator response quality and surrounding road-user interpretability.

Suggested KPIs

- Percentage of mandatory edge-case scenarios successfully completed
- fall-back manoeuvre success rate
- Remote operator response time
- Communication recovery time
- Rate of human-factor-related test failures

3. Define Human-Centred Requirements for Remote Operations

Remote operation centres and supervisory personnel should comply with minimum human-centred operational requirements [14,15,16,20]. addressing:

- Situation awareness
- Workload management
- Alarm prioritization
- Staffing resilience
- Controllability

Compliance Requirements

Compliance criteria should include:

- Mandatory operator certification
- Recurrent competency assessments
- Maximum workload thresholds
- Minimum communication redundancy standards
- Documented organizational safety management procedures

Regulatory authorities should require evidence that remote operators can safely manage:

- Handovers
- Degraded connectivity events
- Simultaneous alerts

This capability should be demonstrated without unacceptable performance degradation.

Suggested KPIs

- Operator training completion rates
- Average alarm acknowledgement time
- Workload exceedance frequency
- Communication uptime percentage
- Successful remote intervention rate
- Operator fatigue-related incident frequency

4. Ensure Predictable and Transparent Driving Behaviour

Automated freight vehicles should demonstrate conservative, predictable, and transparent driving behaviour in mixed traffic environments through measurable behavioural performance benchmarks [3,5,8,12].

Compliance Requirements

Compliance should require validation that vehicles consistently apply:

- Early signalling
- Stable lane positioning
- Conservative gap acceptance
- Socially interpretable manoeuvre execution

These behaviours should be demonstrated across representative traffic conditions.

Authorities should additionally require:

- Standardized external communication protocols
- Behavioural consistency assessments across jurisdictions

These measures would support harmonized public expectations.

Suggested KPIs

- Lane stability deviation metrics
- Signalling lead-time compliance rate

Recommendations

Table 1: Recommendations "Trust, Human Factors and Public Acceptance"

Recommendation for living safety cases for SAE Level 4 Freight operations	
Rec D1.5- 4.	**Recommendation**: Develop continuously updated living safety cases for SAE Level 4 freight operations.
	Motivation: Supports ongoing safety assurance, transparency and trust for evolving ADS
Recommendation for the use of closed-course testing and sandbox	
Rec D1.5- 5.	**Recommendation**: Use closed-course testing and sandbox to validate SAE Level 4 systems before deployment.
	Motivation: Enables safe testing of rare and safety-critical scenarios.
Recommendation for human-centred remote operation development	
Rec D1.5- 6.	**Recommendation**: Develop human-centred remote-operation concepts and procedures.
	Motivation: Human oversight remains essential for safe and scalable operations.
Recommendation for ensuring safe vehicle behaviour	
Rec D1.5- 7.	**Recommendation**: Ensure conservative, predictable and transparent vehicle behaviour.
	Motivation: Predictability and safe fall-back behaviour are key drivers of trust and acceptance.

REFERENCES

1. Kevin Hoff K., & Bashir M. (2015). Trust in Automation: Integrating Empirical Evidence on Factors That Influence Trust. Human Factors the Journal of the Human Factors and Ergonomics Society 57(3):407-434. DOI: 10.1177/0018720814547570

2. Lee J.D.& See K.A.Trust in automation: designing for appropriate reliance Human Factors. 2004 Spring;46(1):50-80. DOI: 10.1518/hfes.46.1.50_30392

3. Bainbridge L (1983). Ironies of automation- Automatica 1983.

4. ISO 21448:(2022). Road vehicles — Safety of the intended functionality Published (Edition 1, 2022). https://www.iso.org/standard/77490.html

5. Rampersad, G., & Kaur, K. (2018). Trust in driverless cars: Investigating key factors influencing the adoption of driverless cars. https://doi.org/10.1016/J.JENGTECMAN.2018.04.006

6. Myklebust T., Stålhane T, GD Jenssen GD., Wærø I (2020). Autonomous cars, trust and safety DOI: 10.1109/RAMS48030.2020.9153618case for the public.2020 Annual Reliability and Maintainability Symposium (RAMS), 1-6, 2020

7. Fraedrich E. and Lenz B.,(2016). Societal and individual acceptance of autonomous driving Autonomous driving, Springer, Berlin, Heidelberg (2016), pp. 621-640

8. Waung M., Mcauslan P., Lakshmanan S. (2021). Trust and intention to use autonomous vehicles: Manufacturer focus and passenger control. Transportation Research Part F Traffic Psychology and Behaviour 80(3):328-340 DOI: 10.1016/j.trf.2021.05.004

9. Tennant C.(2021). Exploring Emerging Public Attitudes Towards Autonomous Vehicles In book: Science Cultures in a Diverse World: Knowing, Sharing, Caring. DOI: 10.1007/978-981-16-5379-7_13

10. Parasuraman, R., & Riley, V. (1997). Humans and automation: Use, misuse, disuse, abuse. Human Factors, 39(2), 230-253. DOI: 10.1518/001872097778543886

11. Ulla Metzger and Raja Parasuraman (2001). Automation-Related “Complacency”: Theory, Empirical Data, and Design Implications. Proceedings of the Human Factors and Ergonomics Society Annual Meeting. Volume 45, Issue 4. https://doi.org/10.1177/15419312010450

12. Madigan R, Louw T., Wilbrink M, Schieben A, Merat N.(2014). What influences the decision to use automated public transport? Using UTAUT to understand public acceptance of automated road transport systems.Transportation research part F: traffic psychology and behaviour 50, 55-64, 201

13. MODI D3.3 Report on User/Driver-Vehicle Interface. 29th September 2023

14. MODI D3.6 Report on safety testing of adapted vehicles and used methods and confidence levels. 9th June 2026

15. Endsley, M.R.(1995). Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors Journal 37(1), 32-64. DOI: 10.1518/001872095779049543

16. Hart & Staveland (1988). Development of NASA-TLX (Task Load Index): Results of Empirical and Theoretical Research. Advances in Psychology.Volume 52, 1988, Pages 139-183

17. ISO 9241-210 (2019. Ergonomics of human-system interaction.Part 210: Human-centred design for interactive systems. https://www.iso.org/standard/77520.html

18. Buysse L., Habli I., Vanoost D. , Pissoort D. (2025).Safe autonomous systems in a changing world: Operationalizing dynamic safety cases. Safety Science. Volume 191, November 2025, 106965. https://doi.org/10.1016/j.ssci.2025.106965

19. Mohammadi N (2019). Towards Preparation for the Trustworthiness Certification using Trustworthiness Cases. In: Trustworthy Cyber-Physical Systems. Springer Vieweg, Wiesbaden.https://doi.org/10.1007/978-3-658-27488-7_13

20. Myklebust T, Stålhane T, Jenssen GD (2023)- Autonomous Vehicles-Trust, Safety and Security Cases: The Complete Picture Annual Reliability and Maintainability Symposium (RAMS), 1-6, 2023

21. Toxtli C.(2025) Human-Centered Automation. ICICT 2025

doi.org/10.48550/arXiv.2405.15960